Cisco Support Tools User Guide for Cisco Unified Software
Release 2.1(1)

June 2007

Table of Contents

List of Figures

Preface

Purpose

This document details the installation, configuration, and day-to-day use of the Cisco Support Tools Server and Cisco Support Tool Nodes.

Audience

This document is intended for System Installers, Administrators, and Users of Cisco Support Tools 2.1(1).

Organization

This document is divided into these parts:

1. Support Tools 2.1(1) Features, Compatibility, and Requirements

2. Support Tools Overview

3. Installing, Upgrading, and Configuring Support Tools

4. Using the Support Tools Dashboard

5. Using Support Tools Web Tools

6. Using Cisco Common Tools

7. Using 3rd Party Tools

8. Reference

9. Support Tools Troubleshooting

Related Documentation

Additional Documents

- *Cisco ICM/IPCC Support Tools Tool Release Notes*

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: - Choose **Edit > Find**. - Click **Finish**.

Convention	Description
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems,Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at **tech-doc-store-mkpl@external.cisco.com** or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems Attn: Customer Document Ordering 170 West Tasman Drive San Jose, CA 95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information. Access the tool at this URL: **http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en**.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only: security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies: psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302

- 1 408 525-6532

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting**show**

command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly

To open a service request by telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

- EMEA: +32 2 704 55 55

- USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) - Your network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) - Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) - Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) - You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Obtaining Additional Publications and Information

Part 1: Support Tools 2.1(1) Features, Compatibility, and Requirements

Chapter 1

New Features in this Release

This release of Support Tools introduces the following new features:

- Support for CVP 4.0: Support Tools is now supported on CVP 4.0 software running, including Audium on AIX. Note that the Audium/AIX installer is only available for CVP versions 4.0 and greater, and is only available as part of the CVP shell installer; a standalone Node installer for AIX is not available. Audium support includes Log Collection and Trace Settings.

- Automated IPSecurity configuration: For Windows 2003 Server platforms, the Support Tools installer includes the option of automatic IPSec configuration. On other platforms, IPSec configuration is not automated but can be configured manually if desired.

- Automated System Addition: The Support Tools Server can now automatically add to its system list nodes defined on CVP 4.x and Support Tools Server 2.1 system lists.

- Cross-version Support Tools Server/Node support: The Support Tools Server and Node are backwards-compatible with previous version of the ST Server and Node.

- Additional Batch Mode scheduling Options: Log collection requests can now be scheduled to run by minutes, days, or weeks.

- Interactive Mode support for Trace Settings and Log Collection: Trace Settings and Log Collection can now be specified in Interactive Mode; logs or trace are performed in real-time against the currently selected system.

- CAD 7.x Trace Support: The Trace Setting tool is now supported for CAD 7.x.

- Millisecond option in Log Collector: For ICM components, dump log data can now be collected in millisecond intervals.

- Additional Merge Log support: Merge Log functionality now supported for CSA, CAD, CRS, and CVP logs.

Chapter 2

Support Tools Requirements and Compatibility

This section contains the following topics:

Support Tools Node Requirements

Support Tools Node Compatibility with Cisco Unified Products and Product Components

The Support Tools Node can be installed on the Cisco Unified components listed below:

Cisco Unified Product or Solution	Supported Versions	Supported Components
Cisco Intelligent Contact Management (ICM) and IP Contact Center (IPCC) Enterprise and Hosted	4.6(2) and above	All
Cisco CallManager (CCM)	3.x, 4.x	All
CTI Object Server (CTIOS)	4.6(2) and above	All
Cisco Unified Contact Center Express (CRS) (formerly IPCC Express)	4.0 and above	All
Cisco Unified IP IVR (CRS)	4.0 and above	All
Cisco Agent Desktop (CAD)	4.6(0) and above	All

Cisco Unified Product or Solution	Supported Versions	Supported Components
Cisco Voice Portal (CVP) (formerly ISN)	2.1 and above	All
Cisco Collaboration Server (CCS)	5.x	All
Cisco E-Mail Manager (CEM)	5.x	All
Cisco Media Blender (CMB)	5.x	All

Support Tools Node Hardware Requirements

The hardware requirements for the Support Tools Node are predetermined by the Cisco Unified software component on which it runs.

The Support Tools Node installation requires a minimum of 20 Mb of available disk space.

Disk space required for log storage is proportional to the number of logs collected and stored. 100 Mb of available disk space is recommended.

Support Tools Node Software Requirements

The software requirements for the Support Tools Node are predetermined by the Cisco Unified software component on which it runs.

Support Tools Server Requirements

Support Tools Server Hardware Requirements

You can install the Support Tools Server on a standalone server (that is, one on which no Cisco Unified products are installed), or on an existing ICM Admin Workstation (AW) in your ICM network. Collocation of the Support Tools Server on other Cisco Unified software product component is not supported.

Warning: Due to possible performance issues, do not install the Support Tools Server on an ICM distributor AW; AW installation should be limited to client AWs.

The Support Tools Server can be installed on these hardware platforms:

- MCS-10-004-Class

- MCS-10-003-Class

- MCS-10-002-Class

- MCS-10-001-Class

Additional hardware requirements include:

- ATA/IDE acceptable

- Graphics card capable of 1024 x 768 x 64K color or better (17" or larger display recommended)

- Disk Space: The Support Tools Server installation uses approximately 100 Mb of disk space. Additional space requirements will depend on the size and quantity of files retained in the Repository at a given time. For typical use, 1 Gb of available disk space is sufficient.

Support Tools Server OS Requirements

Prior to installing the Support Tools Server, one of the following operating systems must be installed and properly configured:

- Microsoft Windows XP Professional with Service Pack 2

- Microsoft Windows 2000 Server with Service Pack 4

- Microsoft Windows 2003 Server Standard Edition with Service Pack 1

Support Tools Server Network Requirements

Ensure that the machine on which you will be installing Support Tools Server has network access and administration rights to each Cisco Unified software component on which the Support Tools Node will be installed.

Support Tools Server / Node Version Compatibility

The Support Tools 2.1(1) Server is backwards compatible with previous versions of the Support Tools Node. The Support Tools 2.1(1) Node is backwards compatible with previous versions of the Support Tools Server. Note, however, that 2.1(1) functionality will not be available when working with earlier versions of the Support Tools Nodes or Server.

Support Tools Port Requirements

Support Tools has the following port requirements.

Support Tools HTTP Server (Tomcat) HTTP and HTTPS Port

Cisco CCBU Support Tools HTTP Server (Tomcat) bundled with Support Tools by default listens for HTTP requests on **port 8188** and HTTPS requests on **port 8189**. These defaults can be changed at installation, if desired.

If a firewall stands between the Support Tools Server and any Support Tools node, and/or between the Support Tools Server and remote users, you must open these ports on the firewall.

Note: Enabling the HTTPS port on a firewall is necessary when using Support Tools in the default HTTPS mode.

Support Tools Listening Port

Support Tools requires a port to initiate connections with and listen for responses between the Support Tools Server and Support Tools Nodes. By default, the Support Tools Server uses **port 39100**. As desired, you can specify a different port during installation.

As part of the Support Tools installation/configuration:

- Ensure that the port used by the Support Tools Server is available on the supported Cisco Unified software products it manages.

- If a firewall stands between the Support Tools Server and any of its ICM or related Cisco Product Nodes, you must open the listening port on the firewall.

- All servers and nodes must use the same listening port. If you change the default port it must be changed on the server and all nodes.

Support Tools Dashboard Web Browser Requirements

Access to the Support Tools Dashboard requires Internet Explorer 6.0 Service Pack 1 or greater. No other browser types are supported.

Warning: While non-supported browsers may appear to work, irregular results can result from their use.

Part 2: Support Tools Overview

Chapter 3

About Cisco Support Tools

Key Features

Cisco Support Tools is an application that contains a suite of utilities that allow you to manage and troubleshoot servers that run broad range of Cisco Unified product software components. Through Support Tools, you can troubleshoot configuration and performance problems on these systems from any machine running a supported version of Windows and Internet Explorer on your network that can access the Support Tools Server.

Access to utilities in the Support Tools suite is through a browser-based interface--the Support Tools Dashboard--installed on the Support Tools Server. Levels of security control both access to the Dashboard and the ability to use specific tools once logged in. In low bandwidth conditions (for example, via dial-up access) or when Web browsing is otherwise impractical, many Support Tools utilities can also be accessed and run via command line.

Key Features

The Support Tools suite includes the standard diagnostic tools delivered with many Cisco Unified products. It also provides key new functionality including the ability to :

- Interrogate individual Support Tools nodes for their hardware/OS, Cisco component, third party product information, and application specific data or files.

- View, stop, and start services running on Support Tools nodes.

- View and terminate processes running on Support Tools nodes.

- Compare and synchronize registry settings from different Support Tools nodes.

- Pull logs from many Support Tools nodes including the following:

  - ICM call routers

- ICM Loggers

- ICM Peripheral Gateways (PGs)

- ICM Admin Workstations (AWs)

- CTI Object Server (CTIOS)

- Cisco Collaboration Server (CCS)

- Cisco Unified Contact Center Express (CRS)

- Cisco Unified IP IVR (CRS)

- Cisco Agent Desktop (CAD)

- Cisco Security Agent (CSA)

- Customer Voice Portal (CVP)

- Cisco Email Manager (CEM)

- Cisco Media Blender (CMB)

- Cisco CallManager (CCM)

- Create enhanced time-synchronized merged logs across different servers.

- Set trace levels trace levels on different applications for a duration of time, then collect logs against that application.

- Run a majority of the tools in either Interactive Mode (where one system is immediately selected and queried) or Batch Mode (where several systems can be scheduled to be queried at some point in the future).

Key Features

About Support Tools Components

Support Tools uses a client/server architecture to support remote systems running Cisco Unified application software. The architecture is comprised of the Support Tools Server and the Support Tools Node. The server and node connect using TCP/IP and can exchange large volumes of messages with only a minimal impact to system performance.

The Support Tools Server

The Support Tools Server must be installed on a system that has little or no performance load, namely a standalone network workstation or a client ICM Admin Workstation (AW). The Support Tools Server can be installed on multiple systems to provide multiple access paths.

Major features of the Support Tools Server include:

- The Support Tools Dashboard, a browser-based interface that allows access to all Support Tools utilities.

- Web Tools-- a set of system management utilities specifically designed for use with Support Tools.

- The Support Tools Repository, a central storage location for history files (for example, logs, registries, etc.) gathered and saved through the Support Tools Dashboard. These files can be downloaded, viewed, and used for system comparison or restoration. Note that multiple installations of the Support Tools Server do not share a common repository--each will maintain its own instance.

The Support Tools Node

The Support Tools Node serves as the client to the Support Tools Server. It is installed on each Cisco Unified product to be managed through Support Tools.

Major features of the Support Tools Node include:

- The Node Agent Service, used to accept connections from the Support Tools Server.

- Command-line versions of most Support Tools utilities, allowing these tools to be run from a node when access to the Support Tools Server is unavailable or otherwise impractical (for example, during a network outage).

- A local Repository used to store saved and downloaded files when Support Tools utilities are run directly from a node (via a command line) outside of the Dashboard interface.

Note: The Support Tools Server installation automatically installs the Node Agent Service to the Support Tools Server, ensuring that this system can also be managed through Support Tools.

About Support Tools Network Topology

The Support Tools Server is installed on a standalone server or a client ICM Admin Workstation in your network. To ensure redundancy, the Support Tools Server can be installed on multiple systems. Note however, these multiple installations do not have the ability to share data with one another.

The Support Tools Server can communicate with Support Tools nodes through a firewall provided the appropriate **ports on the firewall** have been opened.

User access to Support Tools is limited to your network. Remote users wishing to use the Support Tools Dashboard must first connect to the network--remote access via the Internet is not supported.

The following diagram shows Support Tools deployed in a basic IPCC network.

Figure 1: Support Tools Topology
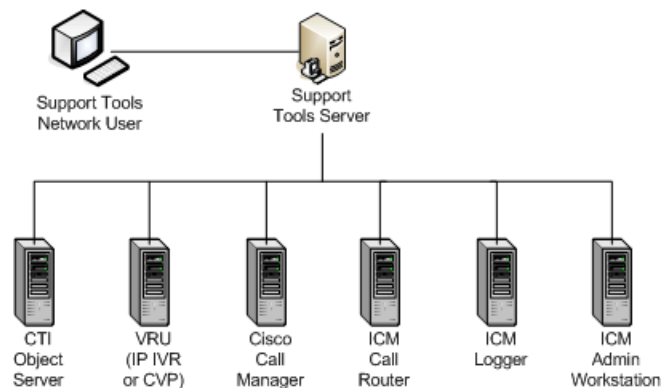
Frequently Asked Questions

This section gives brief answers some to some common questions about Support Tools. All of the subjects addressed here are described in greater detail elsewhere in this guide.

What is the benefit of Support Tools?

Support Tools provides a common interface (the Support Tools Dashboard) to a suite of utilities you can use to examine and troubleshoot Cisco Unified software products.

What components make up Support Tools?

The Support Tools Server provides the engine and interface through which users access Support Tools utilities. The Support Tools Node is the listening agent that allows the Support Tools Server to interact with Cisco Unified software components.

Where do I install the Support Tools Server?

The Support Tools Server can be installed on a client ICM Admin Workstation (AW) or on its own dedicated machine. Do not install the Support Tools Server on an AW Distributor or any other Cisco Unified software component server other than an ICM client AW.

Where do I install the Support Tools node?

The Support Tools node should be installed on each supported Cisco Unified software server that you want to manage with Support Tools. See About Support Tools Platforms for a complete list of supported components.

What performance impact will running Support Tools have on my Cisco Unified system?

Support Tools processes run silently with minimum performance impact.

Note the following with performance in mind:

- Installing the Support Tools Server on its on its own dedicated machine reduces any performance impact that might be imposed if it were collocated with an ICM client AW.

- Because of the possible need to reboot, the Support Tools node should be installed during an off-production maintenance period. Rebooting Cisco Unified software components can cause a loss of service or product functionality.

- Large log collections should be performed at times of low network traffic. Large collections can a spike in bandwidth usage on the system.

- The Support Tools Repository and its subdirectories should be excluded from continuous virus scans.

Who can use Support Tools?

Any Cisco Unified user can use Support Tools with the proper permissions can use Support Tools. Permissions can be set to limit access to certain sensitive utilities in the Support Tools Dashboard to a privileged group.

What configuration does Support Tools require after installation?

While some optional configuration is available (see the Configuring Support Tools section) no post-installation configuration is required to use Support Tools out of the box.

Note: To use Support Tools' merged log capabilities, each Support Tools Server and node must be able to communicate with the same Simple Network Time Protocol (SNTP or NTP) server. See How to Collect Information for a Support Tools Installation for more information.

Frequently Asked Questions

Chapter 4

About Support Tools Utilities

This section describes the different utilities available through Support Tools.

This section contains the following topics:

Support Tools Utilities List

Support Tools includes a suite of utilities to monitor, administer, and configure Cisco Unified software components on which the Support Tools Node is installed. Utilities are grouped into these categories:

- **Support Tools Web Tools**: System Interrogate, Registry, Registry Compare, Processes, Services, Trace, and Log tools, available in both Interactive Mode and Batch Mode.

- **Cisco Common Tools**: Pre-existing Cisco utilities which in most cases already exist on supported Cisco Unified software products as part of a standard installation.

- **3rd Party Common Tools**: Bundled third-party Windows, DOS, and Unix utilities. Windows and DOS utilities will already exist on supported Cisco Unified software products as part of a standard Windows installation. Unix utilities are installed as part of the Support Tools node installation.

Web Tools

The following utilities were created by Cisco specifically for use with Support Tools. They can be run from within the Dashboard interface or from an external command line on either the Support Tools Server or an individual node.

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
Registry	Use to view ICM or related Cisco Product registry entries.	All Windows-based Support Tools nodes	X	
Registry Compare	Use to compare and synchronize ICM or related Cisco Product registry entries.	All Windows-based Support Tools nodes	X	
System Interrogate	Use to display system information (for example, OS, hardware, ICM, SQL).	All Windows-based Support Tools nodes		
Processes	Use to view and stop Processes running on an ICM or related Cisco Product.	All Windows-based Support Tools nodes	X	
Services	Use to view and stop Services running on an ICM or related Cisco Product.	All Windows-based Support Tools nodes	X	

Trace and Log Tools

Support Tools features enhanced logging capabilities including the ability to set trace levels based on existing log groups.

Utility Name:	Description:	Installed On:	Dashboard Privileged Users Only:
Create Log Group	Ability to group a set of servers, products, and processes for which to collect logs.	All Support Tools nodes	
Create Trace group	The ability to set trace levels for a log group.	All Support Tools nodes	

Utility Name:	Description:	Installed On:	Dashboard Privileged Users Only:
Schedule Trace	Schedule the changing of trace levels.	All Support Tools nodes	X
Collect Logs	Collect and view log files from ICM and related Cisco products.	All Support Tools nodes	X

Cisco Common Tools

The following Support Tools utilities were created by Cisco specifically for use with ICM. Most can be run both from within the Dashboard interface, or from an external command line.

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
cicman	Use on a NAM CallRouter to view and set NAM to CICM session information.	NAM Call Routers		
ctitest	Use for debugging or demonstration in a Cisco ICM CTI environment. Can be used in place of an Interactive CTI client application.	CTIOS PGs	X	
dbdiff	Third-party (Microsoft) tool to compare database tables. Invoked with the diffconfig.bat tool.	Nodes on which SQL Server is installed		
dumpcfg	Dump Config ICM audit utility. Use to analyze the ICM Config_Message_Log table. Allows you to determine WHO did WHAT, WHEN, from WHERE, using WHICH program.	Loggers (but can be run from any ICM component)		
icmdba	ICM Database Administration tool. Use to create, monitor, and edit ICM databases, including Logger, HDS, and AWDB databases. ICMDBA is also used to manage various SQL Server operating parameters.	AWs, Loggers (ICM components with DBs)	X	X
mptrace	Use to provide a playback from the Nortel Meridian Automatic Call Distributor (ACD) to troubleshoot potential issues.	MerPim PGs		
nicroi	NIC Remote Operator Interface. Use to configure and debug the (old-style DOS-based) AT&T NIC. Often invoked with the NIC.BAT batch program.	Routers for customers running an AT&T NIC	X	

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
nmstart	Node Manager Start. Use to start an ICM service on a CallRouter, Logger, AW, or PG.	AWs, PGs, Call Routers, Loggers	X	
nmstop	Node Manager Stop. Use to stop an ICM Service on a CallRouter, Logger, AW, or PG.	AWs, PGs, Call Routers, Loggers	X	
opctest	Use to interpret a Peripheral Gateways (PG) status, statistics, etc. It is also possible to enable specific debug tracing in the OPC process.	PGs	X	
procmon	General-purpose debugging tool. Can be used in conjunction with various Network Interface Controller (NIC) and Peripheral Interface Manager (PIM) processes. Use to verify status, set debug trace bits, etc.	PGs, Call Routers	X	
rtrtrace	Use to set various debug tracing on a CallRouter. The additional tracing is output to the .EMS log files, and viewed with the Trace and Log utilities.	Call Routers	X	X
rttest	Use to interpret a Call Router's events and states live without interruption to the running router processes. Rttest has several subroutines that allow viewing status, statistics, etc. It is also possible to enable specific debug tracing in the call router.	Call Routers (but can be run from any ICM component)	X	
ss7nictrace	Use to view and set various debug trace bits on a new style NT SS7 NIC PG.	PGs	X	X
vrutrace	Use to output tracing information from a Voice Response Unit (VRU) device and to and from its PIM process. VRUTrace allows capture and playback of session data.	VRU PGs		

3rd Party Common Tools

The following Support Tools utilities are bundled third-party Windows, DOS, and Unix utilities. Most can be run both from within the Dashboard interface, or from an external command line.

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	No Dashboard or Command-Line Access:
Arp-a	Use to find the media access control address of a host on the same physical network.	All Support Tools nodes		
cat	Use the CAT utility to display, print, and combine files. Equivalent of the DOS type command.	All Support Tools nodes	X	
chmod	Use to change file permissions. Equivalent of the DOS attrib command.	All Support Tools nodes	X	
cp	Equivalent of the DOS copy command.	All Support Tools nodes	X	
df	Use to view disk free information.	All Support Tools nodes		
diff	Use to compare two text files or two directories.	All Support Tools nodes		
du	Use to view disk usage information.	All Support Tools nodes		
fgrep	Use to search for text patterns within a set of files.	All Support Tools nodes		
findstr	Use to find strings in logs or text files. Similar to UNIX's grep command. Useful when parsing log files or other text files to find a snippet of text.	All Support Tools nodes		
grep	Use to search for text patterns within a set of files.	All Support Tools nodes		
head	Use to view user-defined number of lines from the start of a file.	All Support Tools nodes		
IPConfig -all	Use to get host computer configuration information, including the IP address, subnet mask, and default gateway.	All Support Tools nodes		
isql/w	Interactive SQL for Windows. Use to query and update Microsoft SQL Server databases.	Nodes on which SQL Server is installed		X

Support Tools Utilities List

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	No Dashboard or Command-Line Access:
ls	Use to view directory listings. Equivalent of the DOS dir command.	All Support Tools nodes		
mv	Use to move files and directories. Equivalent of the DOS move or rename command.	All Support Tools nodes	X	
NBTStat	Use to troubleshoot NetBIOS name resolution problems.	All Support Tools nodes		
Net Session	Use to view information about all current client sessions with the current system.	All Support Tools nodes		
NetStat	Use to view network information for the current system, including protocol statistics and current TCP/IP network connections.	All Support Tools nodes		
Net Statistics Server	Use to view statistics for the local Server service.	All Support Tools nodes		
Net Statistics Works	Use to view statistics for the local Workstation service.	All Support Tools nodes		
NSLookup	Use to get the IP address and fully qualified DNS of the current system's DNS name server.	All Support Tools nodes		
PathPing	A route tracing tool that combines features of the ping and tracert commands with additional information.	All Support Tools nodes		
ping	Low-level connectivity test. Use to verify end-to-end TCP/IP network infrastructure.	All Support Tools nodes		
pstat	Use to list all NT or Win2K processes, their process ID (PID), memory and cpu utilization, etc.	All Support Tools nodes		
rm	Use to delete files and directories. Equivalent of the DOS delete, recursive del subdirectories commands.	All Support Tools nodes	X	
Route-print	Use to view the contents of the network routing tables.	All Support Tools nodes		

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	No Dashboard or Command-Line Access:
shutdown	Use to shut down a remote host. When used from the Dashboard, shutdown will automatically restart the host after 60 seconds.	All Support Tools nodes	X	
sqlew	SQL Enterprise Manager. Use to monitor and update SQL Server operating parameters, expand databases, etc.	Nodes on which SQL Server is installed		X
stopshut	Use to stop a system from shutting down due to an application or operating system failure.	All Support Tools nodes	X	
strings	Use to find printable strings in a binary file.	All Support Tools nodes		
tail	Use to view user-defined number of lines from end of a file.	All Support Tools nodes		
touch	Use to change the creation date/time for any file.	All Support Tools nodes	X	
tracert	Related to ping command. Use to show each intermediary Hop in the TCP/IP network. Useful in troubleshooting LAN and WAN faults.	All Support Tools nodes		
wc	Use to view a count of characters, words, or lines in a file.	All Support Tools nodes		
which	Use to view the name of the first file encountered while traversing a path or directory tree.	All Support Tools nodes		
winmsd	Windows Diagnostics. Use to gather detailed configuration information about computers running Windows.	All Support Tools nodes		X
NetshDump	Allows you to run the NetShell utility to display or modify the configuration of a currently running computer.	All Support Tools nodes		
Bootcfgqry	Queries Boot.ini file settings.	All Support Tools nodes		

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	No Dashboard or Command-Line Access:
Defraganalyze	Analyzes boot files, data files, and folders on local volumes for fragmentation.	All Support Tools nodes	X	
Defragreport	Reports fragmentation of boot files, data files, and folders on local volumes.	All Support Tools nodes		
Driverquery	Displays a list of all installed device drivers and their properties.	All Support Tools nodes		
Eventtriggers	Displays and configures event triggers on local or remote machines.	All Support Tools nodes	X	
Getmac	Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.	All Support Tools nodes		
Logman	Manages and schedules performance counter and event trace log collections on local and remote systems.	All Support Tools nodes		
Openfiles	Queries or displays open files. Also queries, displays, or disconnects files opened by network users.	All Support Tools nodes	X	
Relog	Extracts performance counters from performance counter logs into other formats, such as text-TSV (for tab-delimited text), text-CSV (for comma-delimited text), binary-BIN, or SQL.	All Support Tools nodes		
SC	Communicates with the Service Controller and installed services. SC.exe retrieves and sets control information about services.	All Support Tools nodes	X	
Schtasks	Schedules commands and programs to run periodically or at a specific time. Adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.	All Support Tools nodes	X	

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:	No Dashboard or Command-Line Access:
SysteminfoTable	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	All Support Tools nodes		
SysteminfoList	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	All Support Tools nodes		
SysteminfoCSV	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	All Support Tools nodes		
Taskkill	Ends one or more tasks or processes. Processes can be killed by process ID or image name.	All Support Tools nodes	X	
TasklistTable	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	All Support Tools nodes		
Tasklist	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	All Support Tools nodes		
TasklistCSV	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	All Support Tools nodes		

Privileged Utilities

Some utilities, when accessed through the Support Tools Dashboard, can only be used by members of the Support Tools privileged user group. If you are not a member of the privileged

user group, these utilities will not appear on the Support Tools Dashboard menu. These utilities include:

- ctitest

- icmdba

- nicroi

- nmstart

- nmstop

- procmon

- registry

- registry compare

- rttest

- shutdown

- upcctest

- processes

- services

Note: These privilege levels only apply to utilities when accessed through the Dashboard; they do not preclude users from running any utility through an independent command line on a node.

Utility Installation Locations

Support Tools utilities exist and can be run from individual supported Cisco Unified software products (note that the Support Tools Server is itself treated as a Support Tools node). When you run one of these utilities through the Support Tools Dashboard, you are actually running the utility remotely on the currently selected node.

Not every utility is installed on every node. For the most part, Cisco Common Tools are installed on core ICM components only: AWs, PGs, Call Routers, and Loggers. For example, CICMan is not present on CVP boxes. See the table in the next section for more information.

If you attempt to launch a utility that is not present on the current system, the Support Tools Dashboard returns a message stating that the command is not recognized.

Non-Dashboard Utilities

Certain ICM and third-party utilities are only available for use through their own GUI; they have no command line access. This also precludes the ability to launch and run these utilities from the Support Tools Dashboard. Note that while these utilities are listed on the Dashboard menu, they cannot in fact be run from there.

These utilities include:

- icmdba

- isql/w

- rtrtrace

- sqlew

- ss7nictrace

- winmsd

Command-Line vs GUI Access

For users who prefer command-lines to GUIs, many Support Tools utilities can also be run from an independent command line. For more information, see the instructions for individual utilities.

Also note that certain utilities (see Non-Dashboard Utilities above) have no command line access. Additionally, **trace** does not have a command line utility. Some **interrogate** features are not supported via the command line interface, specifically the ability to download captured files.

Chapter 5

Interactive Mode vs. Batch Mode

Support Tools supports two primary modes of operation; **Interactive Mode** which is the standard mode to use when querying a single system, and **Batch Mode** which allows you to query several systems at a time for any of the specific tools.

Interactive Mode immediately operates on the currently selected system.

Batch Mode allows you to schedule jobs for multiple systems at any point in the future.

This section contains the following topics:

- Working in Interactive Mode, page 39
- Working in Batch Mode, page 39
- Pending Jobs, page 40

Working in Interactive Mode

Using interactive mode simply involves selecting the system that you want to query using the **Select System** tool, then using any of the tools that fall under the **Interactive Mode** menu.

For some tools, such as System Interrogate, more detail is available in Interactive Mode because the support tools server first queries the selected system to determine the additional types of information that can be retrieved and presents these choices to the user. Whereas in batch mode this cannot be done since several systems of different node types may be queried during a batch mode process, and there is no user-intervention to select specific results from a server query.

Working in Batch Mode

Batch Mode allows you to query several servers at once by scheduling a tool to run at any time in the future.

Using Tools in Batch Mode

To use a tool in batch mode:

Step 1   Select a tool to use that is within the **Batch Mode** menu.

Step 2   Schedule a time to run the tool. Enter a Date and Time using the calendar at the top of the page for the selected Batch Mode tool.

Note: You must select a time in the future.

Step 3   Check the select boxes next to the Systems on which you want use this tool.

Step 4   Click **Schedule** to schedule the Batch Mode operation.

A page appears confirming that the batch job has been scheduled.

Step 5   Click **OK**.

You are returned to the Batch Mode scheduling screen for the selected tool.

Note:

- You can view the results of batch mode operations for any given tool by selecting **History** under that tool in the **Batch Mode** node of the Support Tools menu.

- You can view **Pending Jobs** for any given Batch Mode tool by selecting the **Pending Jobs** node under that tool in the **Batch Mode** node of the Support Tools menu.

- A separate batch job is created in the **Pending** list for each system that is selected.

Pending Jobs

The **Pending Jobs** screen displays a list of jobs that are schedule to run for the selected Batch Mode tool.

You can click **Refresh** at any time to see if any new jobs have been scheduled or started.

Note: If you schedule a job in the short future (~ 2 minutes) then the job may not appear in the Pending Jobs prior to its execution.

Canceling a Batch Mode Job

You can cancel any pending job for a batch mode tool. To cancel a pending job:

Step 1   Check the select box(es) next to the scheduled time of a pending job.

Step 2   Click **Cancel**.

A confirmation dialog box appears.

Step 3   Click **OK** in the confirmation dialog box.

Step 4   Click **OK** to return to the Pending Jobs screen.

Pending Jobs

Chapter 6

About Support Tools Security

Support Tools Security Features

Support Tools operates with the following security features/restrictions:

1. Access to Support Tools is limited to the local network. Remote access via the Internet is not supported. Users must authenticate against the network in order to use Support Tools.

2. Users must login to the Support Tools Dashboard using their network ID and password, or the ID and password of a valid Windows account.

   Note: The Support Tools Login page uses SSL by default so that user passwords and all communication between the server and the web client are encrypted and secure.

3. Within the Support Tools Dashboard, access to specific utilities is determined by Windows User Group membership. Only members of the user group designated as the Support Tools privileged group can use utilities capable of system modification from the Dashboard. Non-privileged users are limited to information gathering functionality only. Note that Support Tools utilities used outside of the Dashboard environment (namely, via command-line) do not impose these levels of privilege.

   The use of Support Tools utilities outside of the Dashboard environment (accessed via command line interface on a node) is not controlled by a login/password. System administrators can use Windows privileges to limit this method of access to specific users or groups.

4. Optionally, to enhance security, on Windows 2003 systems, you can use Support Tools' automated deployment of IPSecurity to authenticate requests from the Support Tools Server to a node. Automated IPSec setup is not available on non-Windows 2003 systems, but IPSec can be configured manually, if desired.

Using IPSecurity with Support Tools

Optionally, you can use IPSecurity to secure communication between the Support Tools Server and Support Tools Nodes. Authentication occurs at the Node when the Support Tools Server makes a request. As such, an IPSec-secured Support Tools Server can make requests to an unsecured Node, but a secured node will not accept requests from an unsecured server.

The Support Tools Server uses a client-policy with a filter that requests security. The Support Tools Node uses a client-policy that requires security. The filter does not monitor one-to-one connections. Instead, the filter monitors all incoming IP traffic that uses the default Support Tools TCP Port (39100). The Support Tools Server, by requesting but not requiring IPSEC from each Node, does not deny traffic from a Node that is unable to use IPSEC.

Support Tools uses the ESP protocol (Encapsulating Security Payload) for authentication but does not use encryption. ESP is used to authenticate instead of the AH protocol (Authentication Header) for the ability to support NAT.

Support Tools uses SHA1 for the integrity algorithm in ESP. The policy uses preshared keys.

Automated IPSec Implementation

On Windows 2003 Server machines, Support Tools gives you the option of using an automated implementation of IPSec.

Support Tools implements IPSec as follows:

- You specify the IPSec preshared authentication key to use during Support Tools Server and Node installation. Keys are case-sensitive and limited to 256 characters. Any character except single and double quotation marks, back slash, and pipe can be used.

  Note: For Cisco Unified products that include a bundled install of the Support Tools Node (e.g., CVP 4.0), leaving the IP Shared Key value unspecified during installation may cause Support Tools to install disabled. When this occurs, to enable the node you must manually start the Node Agent Service on the target machine.

- Authentication occurs at the Node when the Support Tools Server makes a request. As such, an IPSec-secured Support Tools Server can make requests to an unsecured Node, but a secured node will not accept requests from an unsecured server.

- During installation, Support Tools only prompts for a preshared key when a security policy can be created and assigned. Support Tools creates a security policies subject to these conditions:

  – If a Cisco policy already exists on the target machine (whether assigned or not) Support Tools will not create a new policy.

  – If a non-Cisco policy already exists on the target machine and is assigned, Support Tools will not create or assign a Cisco policy.

    – If a non-Cisco policy already exists on the target machine and is not assigned, Support Tools will create and assign a Cisco policy.

Manual IPSec Implementation

On Windows 2000 and XP platforms, IPSec can be used but must be configured manually. This section provides guidelines on setting up IPSec for Support Tools.

When configuring Support Tools to use IPSec:

- The policy for the Support Tools server should be configured to support shared keys.

- A filter should be added complying with the above listed recommendations when securing a Support Tools component that resides on a system with a one-to-one IPSEC policy. The filter should be added to the filter list of the existing policy and listed second.

A configuration example follows:

```
Client Policy
 IP Filter
  From any IP address / TCP port
  To any IP address / specific TCP port (39100, Support
Tools default)
 Filter Action
  Request Security on Support Tools Server
  Require Security on Node Agent
   Negotiate security
    ESP with SHA1 Integrity and no encryption
 Authentication Mode (Both should be listed on Support
Tools server)
  Preshared key
```

Using IPSecurity with Support Tools

Part 3: Installing, Upgrading and Configuring Support Tools

Chapter 7

Installing Support Tools

This section contains the following topics:

About Installing Support Tools

Installing Support Tools consists of:

1. Installing the Support Tools Server to a central server with access to your ICM system. Optionally, you can install the Support Tools Server on multiple servers to provide multiple access paths. Note, however, that data is not shared between these separate installations.

   Note: The Node is automatically included in the Support Tools Server installation; a separate installation of the node on this machine is not required.

2. Installing the Support Tools Node on each ICM or related Cisco Product to be managed from the Support Tools Dashboard.

Support Tools Installation Tasks

To install Support Tools, follow the sequence of steps in the checklist below. Each of these steps is described in greater detail in following sections. Review this list before proceeding with the installation.

> **Note:** Before proceeding with installation, also be sure to review the Support Tools Release Notes for any updates pertaining to Support Tools installation. The Release Notes are available at the top level of the Support Tools CD and at **http://www.cisco.com**.

> **Warning: In some instances, the Support Tools Server and Node installation may require a reboot to complete. For this reason, you should perform the installation during a regular maintenance period when the machine is in off-production mode.**

Table 1: Steps for Installing Support Tools

Collect information for the install (page 51).   Prior to installing Support Tools, collect the information that you will need to provide during the install.
Create the Support Tools privileged user group (page 53).   Create and assign users to the Windows user group that will serve as the Support Tools privileged user group.
Create the Distinguished User Account (page 53)   The Support Tools Server installs the Tomcat Web server which runs as a service called "Cisco CCBU Support Tools HTTP Server." This service must run as a distinguished user. To do this: 1. Prior to installing the Support Tools Server, create the Distinguished User account.   2. After installing the Support Tools Server, assign the Distinguished User the requisite directory privileges.
Review the Support Tools Server hardware and software prerequisites   Prior to installing the Support Tools Server, ensure that the machine you are installing it on meets the minimum hardware and software prerequisites.
Install the Support Tools Server   The Support Tools Server installation includes: • The Support Tools Dashboard   • The Support Tools Node   • Support Tools documentation   • Java Virtual Machine (JVM) 1.5.0_05   • Apache Tomcat 5.5.16
Review the Support Tools Node hardware and software prerequisites   Prior to installing the Support Tools Node, ensure that the supported Cisco Unified software products you are installing it on meet the minimum hardware and software prerequisites.

Install the Support Tools Node

Install the Support Tools Node on each ICM or related Cisco Product you want to manage through Support Tools. The Support Tools Nodes installation includes:

- The Support Tools Node Agent Service

- Support Tools Web utilities and certain Unix-style 3rd Party Common Tools.

- Support Tools documentation

Note: Other Support Tools utilities are not part of the Support Tools installation. Rather, these utilities already exist on each node, distributed as part of standard ICM and Windows installations.

Enable ports for Support Tools

Support Tools uses the following ports:

- Tomcat (the **Cisco CCBU Support Tools HTTP Server**) by default listens for HTTP requests on port 8188. It listens for HTTPS requests (used for SSL) by default on port 8189.

- Support Tools requires a port (39100 by default) to communicate between the Support Tools Server and Nodes. Ensure that this port is available on each node managed by Support Tools.

If a firewall stands between the Support Tools Server and any Support Tools node, and/or between the Support Tools Server and remote users, you must open these ports on the firewall.

Test the installation

After installing Support Tools, perform a few simple tests to verify that the install was successful.

Post-Installation Configuration

All basic configuration required by Support Tools is set during installation. Immediately after installation, no further configuration is necessary to begin using the product.

However, as desired, after installation you can modify the settings chosen during installation, or use certain optional behaviors that require further configuration.

How to Collect Information for Support Tools Installation

Prior to installing Support Tools, collect the following information that you will need to provide during the install

---

Step 1   For the Support Tools Server

a. Determine the name of the Support Tools **privileged user group**. Determine which users will be members of this group.

b. Determine the username, domain, and password of the distinguished user (page 53) for the Cisco CCBU Support Tools HTTP Server.

c. Determine the IP address or fully-qualified DNS of your network time server.

To use Support Tools **merged log capabilities**, each Support Tools Server and node must be able to communicate with the same Simple Network Time Protocol (SNTP or NTP) server. This is required even for networks that have fully synchronized Windows 2000/2003 systems as the allowable machine drift is greater than the tolerance of the log event times.

Note that Support Tools does not make time adjustment to host machines. Instead, the time offsets are tracked in a database to use for log merging only. Your SNTP or NTP server must support unauthenticated requests. Refer to RFC-2030 for more details on SNTP. Most Cisco IP Routers support the SNTP / NTP protocol. Consult with your IT department on available SNTP / NTP servers in your network.

If any system in a merged log collection cannot communicate with the SNTP server, the merge will fail, and the outputted log will contain the alert: "Missing SNTP data for all of the following files logs prevented merging logs:..."

Step 2   For the Support Tools Node

a. Take an inventory of the **supported Cisco Unified software products** on which you want to install Support Tools.

b. Determine the IP address or fully-qualified DNS of your network time server (SNTP). However, you can leave this blank if the SNTP address was filled in on the Support Tools Server. The Support Tools Server pushes the value out to the node. Note that this only occurs if the SNTP server field is blank. If a value is pushed to the node and the address later changes, you must manually change the address on the Support Tools Node to point to the new SNTP server.

c. Determine whether a **firewall** stands between the Support Tools Server and any supported Cisco Unified software products it will manage. If so, open the required ports.

How to Create Support Tools User Groups

Support Tools recognizes two categories of users:

- *Privileged* users have full access to all Support Tools functionality, including tools and commands that can be used to modify system settings, registries, etc.

- *Regular* users have limited access to information gathering functionality only. Tools capable of system modification are not available to regular Support Tools users.

To Create Support Tools User Groups

Support Tools assigns privilege based on regular Windows user groups. This can be either a local group you define on the Support Tools Server machine or a domain group you define using Active Directory.

During the Support Tools Server installation, you are prompted to enter the name of one (and only one) Windows user group that will serve as the Support Tools privileged group. Users in all other groups are treated as regular Support Tools users.

Note:

- The privileged user group name is case-sensitive. It must match in case its corresponding Windows user group name.

- All Support Tools users must be members of the Windows Everyone group; anonymous users will not have access to Support Tools.

After installation, if necessary, you can modify the privileged group name by running the **Support Tools Server configuration**.

Creating Local Accounts on the Support Tools Server

To ensure you have local access to the Support Tools Dashboard in situations when network authentication is unavailable (for example, due to a downed network or authentication server) it is a good idea to create one or more local user accounts on the Support Tools Server.

To ensure full access to all utilities, these local accounts should be made members of a local user group named identically to your Support Tools privileged user group.

When logging into the Dashboard using a local account, enter <hostname>\<Windows_username> as your username; for example, `my_server\my_username`.

How to Create the Distinguished User Account

The Support Tools Server installs the Cisco CCBU Support Tools HTTP Server (Tomcat) which runs as a service. This service must run as a distinguished user. To do this:

1. *Prior* to installing the Support Tools Server, create the Distinguished User account as described below.

2. *After* installing the Support Tools Server, assign the Distinguished User the requisite directory privileges as described below.

How to Create the Distinguished User Account

Before installing the Support Tools Server, on the machine on which the Support Tools Server will be installed, create a local or domain account to be used for the Cisco CCBU Support Tools HTTP Server (Tomcat) service.

Note: This account is only used to run the Cisco CCBU Support Tools HTTP Server (Tomcat) Service and should not be an administrator or user account for any other purpose. Create a local account since this will restrict access of the Cisco CCBU Support Tools HTTP Server (Tomcat) Service to the one machine. In some scenarios using a local account for the service will prevent users from authenticating with a domain account. If this condition exists, you will need to use a domain account instead.

How to Assign Directory Privileges to the Distinguished User

If your Support Tools Server uses NTFS directory security that limits directory access to specific users, after installing the Support Tools Server, ensure that, in addition to the <machine>\System account, the distinguished user for the Cisco CCBU Support Tools HTTP Server (Tomcat) Service has the following privileges to the Support Tools root directory and all of its subdirectories:

- Modify

- Read & Execute

- List Folder Contents

- Read

- Write

For example, If the Distinguished User specified during installation is `my_domain\tomcat_svc_acct`, then my_domain\tomcat_svc_acct must be given the rights listed above to the Support Tools root directory and all of its subdirectories.

See your Windows documentation for instructions on granting NTFS security privileges.

How to Install the Support Tools Server

You can install the Support Tools Server on any server with access to your ICM system. Before installing the Support Tools Server, ensure that the machine meets the **prerequisite hardware and software requirements**.

Warning: In some instances, the Support Tools Server and Node installation may require a reboot to complete. For this reason, you should perform the installation during a regular maintenance period when the machine is in off-production mode.

The Support Tools 2.1(1) CD includes a Server Install Wizard that installs:

- The Support Tools Dashboard

- The Support Tools Node

- Support Tools documentation

- Java Virtual Machine (JVM) 1.5.0_05

- Apache Tomcat 5.5.16

Note: The installation instructions below describe only those installer dialogs that require user input.

Step 1   Log into the machine on which you are installing the Support Tools Server under an account with local Windows Administrator privileges for that machine.

Step 2   If the Cisco Security Agent is running on the machine, stop its service and set the service startup type to Disabled.

Step 3   Insert the Support Tools CD in the server's CD-ROM drive. Normally an autorun executes and you can skip the next two steps.

Step 4   If the autorun does not execute, from the Windows Start Menu, select Run.

Step 5   Browse to and double-click the Support Tools Server executable file located at: `Server\setup.exe`.

Step 6   If the installer detects a previous, earlier installation of the JVM (less than 1.5.0_05), you will be prompted to confirm an overwrite. Click Yes.

Step 7   Specify values for each of the following:

- Destination Path: Specify the location to install the Support Tools Server, or accept the default: c:\Cisco\CCBU\SupportTools. You can install the Support Tools Server to any location on the local machine.

  Note: If you plan on using the Cisco Security Agent (CSA) you can only change the drive letter and must leave the remaining default path information. This is because CSA security rules are written specifically based on the path names.

- Administration Group Name: The name of the **Windows User Group** that has access to Support Tools functions capable of system modification (non-administration group users can use Support Tools for information gathering only). The default is Administrators.

> **Note:** The Administration Group name is case-sensitive. It must match in case its corresponding Windows user group name.

- Domain, Username, and Password of user that the Cisco CCBU Support Tools HTTP Server (Tomcat) should run under. For more information, see **How to Create the Distinguished User Account**.

> **Note:** Use the **Test** button to test Authentication.

- TCP/IP Port: The port the Support Tools Server uses to communicate with Support Tools Nodes. The default is 39100.

- HTTP and HTTPS Ports: Specify the ports that the Cisco CCBU Support Tools HTTP Server (Tomcat) should use for HTTP and HTTPS requests. The Support Tools defaults are 8188 (HTTP) and 8189 (HTTPS).

- Network Time Server: Specify the static IP address or fully-qualified DNS of your network time server. Also specify the frequency (in minutes) with which this machine should reconcile its clock against the network time server. Will network time server usage is optional, without it merged logs cannot be collected.

> **Note:** As necessary, these values can also be modified after installation.

- Repository Base Directory: Specify the path to the Support Tools Server Repository. This is the location where log files and saved registries and processes lists are stored. You can specify any location on the Support Tools Server's physical drive. The default is <destination_path>\Repository.

- IPSec Preshared Key: For Windows 2003 installs only, you have the option of entering an IPSec key that authenticates the Support Tools Server to individual nodes. Keys are case-sensitive and limited to 256 characters. You can use any character except single and double quotation marks, back slash, and pipe.

> **Note:** If an IPSec policy is already assigned on you machine, you will not be prompted to enter a preshared key. For more, see Automated IPSec Implementation (page 44).

Step 8   When the installation is complete, click Finish.

Depending on your local machine's configuration, you may be prompted by the installer to reboot the machine to complete the installation. The Support Tools Server and Cisco CCBU Support Tools HTTP Server (Tomcat) services will start automatically upon reboot.

Step 9   If you are not prompted to reboot, the Support Tools Server and Cisco CCBU Support Tools HTTP Server (Tomcat) services will start automatically and is ready for use.

Step 10   If you stopped the Cisco Security Agent for the installation, start its service and set the service startup type to Automatic.

How to Install the Support Tools Node

You can install the Support Tools Node on any supported Cisco Unified software component that you want to manage through Support Tools.

Note: Before installing the Support Tools Node, ensure that the machine meets the **prerequisite hardware and software requirements**.

Warning: In some instances, the Support Tools Server and Node installation may require a reboot to complete. For this reason, you should perform the installation during a regular maintenance period when the machine is in off-production mode.

The Support Tools CD includes a Server Install Wizard that installs:

- The Support Tools Dashboard

- The Support Tools Node

- Support Tools documentation

Note: The installation instructions below describe only those installer dialogs that require user input.

Step 1 Log into the machine on which you are installing the Support Tools Server under an account with Windows Administrator privileges.

Step 2 If the Cisco Security Agent is running on the machine, stop its service and set the service startup type to Disabled.

Step 3 Insert the Support Tools CD in the server's CD-ROM drive. Normally an autorun executes and you can skip the next two steps.

Step 4 If the autorun does not execute, from the Windows Start Menu, select Run.

Step 5 Browse to and double-click the Support Tools Node executable file located at: nodes\setup.exe.

Step 6 Specify values for the following:

- TCP/IP Port: The port the Support Tools Server uses to communicate with Support Tools Nodes. The default is 39100.

- Destination Path: Specify the location to install the Support Tools Node, or accept the default: c:\Cisco\CCBU\SupportTools. You can install the Support Tools Node to any location on the local machine.

> **Note:** If you plan on using the Cisco Security Agent (CSA) you can only change the drive letter and must leave the remaining default path information. This is because CSA security rules are written specifically based on the path names.

- Network Time Server: Specify the static IP address or fully-qualified DNS of your network time server. Also specify the frequency (in minutes) with which this machine should reconcile its clock against the network time server.

  > **Note:** As necessary, this value can also be modified after installation.

- IPSec Preshared Key: For Windows 2003 installs only, you have the option of entering an IPSec key that authenticates the Support Tools Server to individual nodes. Keys are case-sensitive and limited to 256 characters. You can use any character except single and double quotation marks, back slash, and pipe.

  > **Note:** If an IPSec policy is already assigned on you machine, you will not be prompted to enter a preshared key. For more, see Automated IPSec Implementation (page 44).

Step 7 When the installation is complete, click Finish.

Step 8 Depending on your local machine's configuration, you may be prompted by the installer to reboot the machine to complete the installation. The Support Tools Node will start automatically upon reboot.

Step 9 If you stopped the Cisco Security Agent for the installation, start its service and set the service startup type to Automatic.

How to Test the Support Tools Installation

After installing Support Tools, you should test your installation by:

- Accessing the Support Tools Dashboard.

- Testing the connection to Support Tools Nodes.

Step 1 Access the Support Tools Dashboard

    a.   Open a Web browser and in the Address line, enter: `http://<hostname_or_ip_address>:<Tomcat_HTTP_port>`.

> **Note:** The Cisco CCBU Support Tools HTTP Server (Tomcat) default http port is 8188. This default can be modified during installation.

    b.   Press <Enter>. The Support Tools Dashboard Login screen opens.

    c.   In the Login Name field, enter `<Windows_domain>\<Windows_username>`. For example, `my_domain\my_username`.

    d.   In the Password field, enter your Windows password (case-sensitive)

      e.   Click Login.

Step 2   Test the Connection to a Support Tools Node

      a.   On the System Management screen, add the node(s) you want to test to the system list.

      b.   On the System Management screen, use the Test Connection utility to confirm the connection to individual nodes.

How to Create the Distinguished User Account

Chapter 8

Configuring Support Tools

This section contains the following topics:

About Configuring Support Tools

All basic configuration required by Support Tools is set during installation. Immediately after installation, no further configuration is necessary to begin using the product.

However, at some point you may want to modify the settings chosen during installation, or use certain optional behaviors that require further configuration.

These post-installation configuration options include:

- **Modifying the basic Support Tools setting specified during installation** (network time server, privileged use group, Repository path, and TCP/IP port).

- **Excluding the Support Tools Repository from continuous virus scans.**

- **Installing Windows Management Instrumentation (WMI) on Cisco Unified Nodes running SQL 2000** so that this information can be reported on by the Support Tools System Interrogate utility.

- **Adding information about specific processes and services that display in the Processes & Services screen.**

How to Modify Support Tools Basic Configuration

The basic configuration settings necessary to run Support Tools (network time server, privileged use group, Repository path, and TCP/IP port) are specified during installation. While not typically necessary, you can modify these settings after installation.

Support Tools keeps most of its configuration values in the Windows Registry. The base key for all values is: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools.

Note: After modifying any of the following settings you must restart Support Tools services for the change to take effect.

Communication Port

The ports the ST processes use are defined in the Windows registry at the following DWORD value: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\Port

Location of the Support Tools Installation

This value is stored in the Windows registry in: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\InstallPath. This can be changed in the registry, but you must manually move the directory on the file system to the new location.

Location of the Support Tools Repository

This value is stored in the Windows registry in: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\RepositoryBaseDir. This can be changed in the registry, but you must manually move the directory on the file system to the new location. The repository location must be on a local disk (i.e., it cannot be on a network share).

Support Tools Administrative Group

This value is stored in the Windows registry in: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\Privileged Group\GroupName.

Tomcat Designated User

Account information for the Tomcat Designated User (user name, domain) is stored in the Windows registry in: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\DistinguesdDomainName and HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\DistinguesdUserName.

Note: The password for the Designated User is not stored in the registry. It must be modified (if desired) via the Windows User Panel.

TCP/IP Port

(should never be changed) This value is stored in the Windows registry in: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CCBU\Support Tools\AppServer\Port This value can be changed, but it must be changed to the same value on all Support Tools Servers and Nodes.

How to Disable Continuous Virus Scan for the Repository

Support Tools writes a large number of files (.log, .txt, .xml, and .zip) to the Repository in the course of normal use. The quantity of these files, if used in conjunction with continuous virus scanning, could result in a negative impact on performance.

If this performance degradation is not acceptable then you can restrict continuous virus scanning in the Repository directory and its subdirectories to known file types only (which should omit .log and .txt files from scanning).

If performance degradation persists, then :

- Exclude the Repository directory and its subdirectories from continuous virus scans run on the Support Tools Server and Node machines. Instead, limit scans on these directories to a nightly basis.

- After disabling virus scanning for the Repository directory and its subdirectories, use NTFS directory security to limit full access to these directories to administrators, NT Authority\System, NT Authority\Service and any other distinguished users that require direct access to these directories.

Warning: Steps A and B above should be used in concert with each other; that is, do not disable continuous virus scanning without also implementing NTFS directory security on the affected directories.

The default location of the Support Tools Repository on both the server and node is `<support_tools_root>\Repository`.

How to Modify Processes and Services Listed in the Process Information List

The process information list stores information about specific processes and services. The information from this file is then displayed to Support Tools users when they use the Processes and Services utility.

For each process or service defined therein, the file includes:

- The name of the process or service

- Whether the process is known, unknown, or critical

- Explanatory text about the process

Out-of-the-box, the process information list includes information on the following processes:

- All Cisco processes are identified as Known.

- Certain critical Microsoft OS-related processes are identified as Critical.

- Certain SQL and common Microsoft processes are identified as Known.

As desired, you can modify the process information list to add new information about processes or services. For example, if you are running a virus checker, you may want to tag it as critical.

Note:

- Services are listed only if they have a known name. The known name is derived from the .exe file name of the service. For example, the process named "tomcat.exe" is also the service "Cisco Support Tools HTTP Service". Prior to making additions or modifications of a service be sure to correlate the .exe file name of the service with the service name.

- Do not modify **systemlist.xml** file. Changes to this file are not supported by Cisco.

Step 1 Use a text editor to open **processinfo.xml** located on the Support Tools Server at **<support_tools_root>\repository\system files**

Note: Only the processinfo.xml file on the server needs to be modified. The server pushes the modified file out to all Support Tools nodes connected to the server.

If you have multiple Support Tool Servers then you should make the same modifications to all servers if the servers connect to the same nodes. Otherwise the **processinfo.xml** on the nodes may be different, depending on which server they are currently connected.

Step 2   Using proper well-formed XML syntax, add or modify entries as follows:

- Process Type: Known, Unknown or Critical. Note: Use only these designations. Others will not parse correctly. Designating a process as Critical will prevent Dashboard users from stopping it (on the Services screen).

- Name: The name of the process or service. Can include, but does not require, an .exe extension.

- Manufacturer: Optionally, the manufacturer of the process or service.

- Help: Any explanatory information you wish to display about the process or service.

- Example: `<process type="known" name="notepad.exe" manufacturer="Microsoft"><help>This is Microsoft's Notepad text editor</help>`

When editing the file, consider the following:

- Cisco processes and services not identified in processinfo.xml are nonetheless automatically detected by the Processes and Services utility and labeled as Known.

- Non-Cisco processes and services not identified in processinfo.xml are labeled as Unknown.

- Be aware that Support Tools Dashboard users will be unable to stop services and processes tagged Critical.

- Consider that there is value in leaving less important processes and services tagged as Unknown. It allows Support Tools users to bulk select these items for termination when troubleshooting a node.

- Be careful to use correct XML syntax when editing the file. Incorrect syntax makes the file unreadable to the Support Tools parser, causing all but Cisco processes and services to display as Unknown.

The current processinfo.xml file is automatically propagated from the Support Tools Server to individual Support Tools nodes when these systems are selected for use from the Dashboard. In this way, an updated version of the file is available to users who launch the Processes and Services utility directly from a node via command line.

Note however that there may be instances where you may want or need to manually copy an updated processinfo.xml file from the Support Tools Server to another machine: for example, if you are running multiple installations of the Support Tools Server, or if you have nodes that are rarely selected for use from the Dashboard, but on which users may run the Processes and Services utility from a command line.

How to Configure SQL for Use with the System Interrogate Tool

In order for the Support Tools System Interrogate utility to access and report on an ICM system's SQL database information, it must have access to Microsoft's Windows Management Instrumentation (WMI). WMI is not part of a standard Windows SQL install, and in most cases will therefore need to be installed separately. To Install WMI:

Step 1   Obtain the SQL 2000 Server CD, or download WMI at: **http://msdn.microsoft.com/downloads/list/wmi.asp**

Step 2   On each ICM system that has SQL installed (and with which you want to use the System Interrogate utility--(for example, loggers, AWs) run setup from the `\x86\OTHER\wmi` directory.

Note: For additional information on installing and using WMI, see the MSDN library at: **http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/sql_for_wmi.asp**

Configuration of sysquery and Trace

The sysquery and trace configuration files also exist on the Support Tools Server. However these files should **not** be modified. Modifications to these files are not supported. If modifications are deemed necessary by Cisco Systems Inc., then updates will be made available using the patch process.

Chapter 9

Uninstalling, Reinstalling and Upgrading Support Tools

This section contains the following topics:

How to Uninstall Support Tools

As desired, you can uninstall the Support Tools Server or Node by following the steps below. Note that it is not necessary to uninstall either as a precursor to reinstalling the product. This topic describes how to uninstall the Support Tools Server and the Support Tools Node.

Warning: If you are running a patched version of Support Tools (e.g., 2.1(2), 2.1(3) you must back out all installed patches prior to uninstalling the your base version of Support Tools. Use Windows Add/Remove programs to remove patches. using the Patch Manager uninstallation utility. To confirm the version and build number of your Support Tools Server, On the Dashboard menu, select Support Tools. Your version information displays under Support Tools Dashboard.

Step 1   To Uninstall the Support Tools Server

Uninstalling the Support Tools Server removes the Support Tools Server, its associated utilities, and registry entries associated with Support Tools. Note that uninstalling the Support Tools Server does not automatically remove the Repository files.

    a.   From the Windows Start menu, select Settings > Control Panel > Add/Remove Programs > Cisco Support Tools.

    b.   Click Remove.

c. The uninstaller will ask if you want to remove everything. Select Yes.

d. If desired, after running the uninstaller, use Windows Explorer or a similar file management tool to delete the Support_Tools directory.

Step 2 To Uninstall the Support Tools Node

Uninstalling the Support Tools Node removes the Node only--it does not remove utilities or other items that are part of a standard ICM installation.

a. From the Windows Start menu, select Settings > Control Panel > Add/Remove Programs > Cisco Support Tools.

b. The uninstaller will ask if you want to remove everything. Select Yes.

c. If desired, after running the uninstaller, use Windows Explorer or a similar file management tool to delete the Support_Tools directory.

After removing Support Tools from an ICM or related Cisco Product Node, you should also remove that node's entry in the Support Tools System List (in the Support Tools Dashboard).

How to Reinstall Support Tools

As desired, you can re-install the Support Tools 2.1 Server or Node, using the same steps employed for an initial installation.

Warning: Prior to re-installing Support Tools 2.1, you must uninstall it following the uninstallation instructions in this guide. Failing to uninstall Support Tools prior to a reinstall can cause problems with IPSec functionality (see Troubleshooting).

Upgrading Support Tools

You upgrade support tools simply by running the appropriate Support Tools 2.1(1) installer (Server or Node) on a machine with an existing Support Tools Server or Node. The Support Tools Repository remains intact and saves the files from your previous version of support tools.

You can optionally upgrade from a Node to a Server. The installation program asks you if you are sure that you want to follow one of these upgrade methods so that you do not mistakenly upgrade a Node to a Server or a Server to a Node.

Part 4: The Support Tools Dashboard

Chapter 10

Using the Support Tools Dashboard

The Support Tools Dashboard is a browser-based interface that allows you to access and use all Support Tools utilities through a single interface. The Dashboard integrates access to all Cisco Unified software components where the Support Tools Node has been installed, eliminating the need to manually connect to each remote system.

Figure 2: Support Tools Dashboard
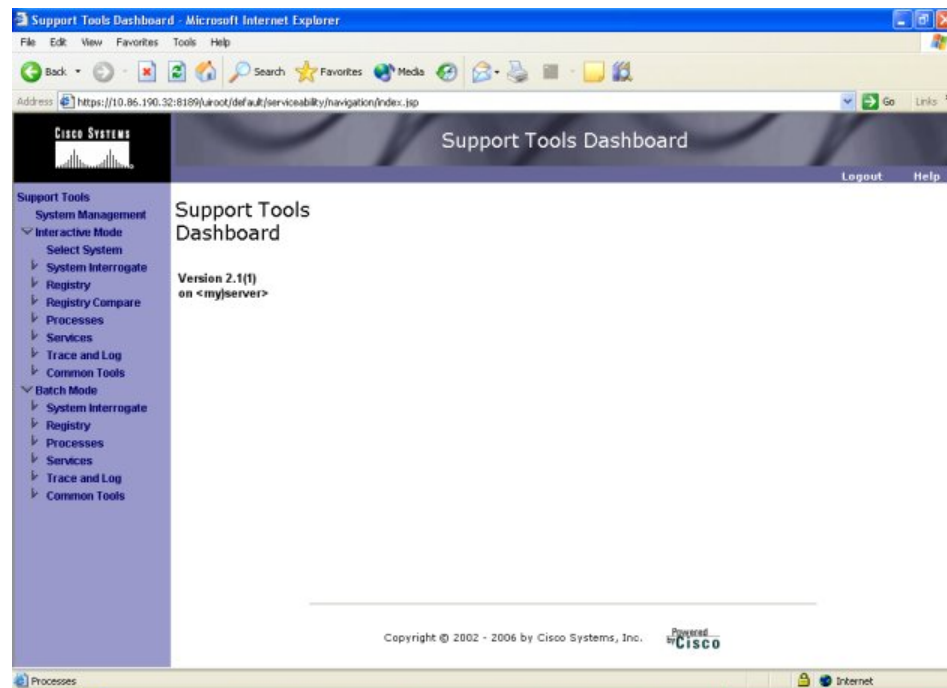
This section contains the following topics:

- Accessing the Dashboard and Privileges, page 72
- Using the Dashboard for the First Time, page 72
- How to Access the Support Tools Dashboard, page 74

Accessing the Dashboard and Privileges

Accessing the Dashboard

Users access the Dashboard via a URL (`http://`

`<hostname_or_ip_address>:<support_tools_port>/`[1]) entered in a browser window. Upon connecting, users must login by providing their Windows user name and password, or the user name and password of a privileged account.

Dashboard Privileges

The Support Tools Dashboard recognizes two categories of users:

- *Privileged* users have full access to all Support Tools functionality, including tools and commands that can be used to modify system settings, registries, etc.

- *Regular* users have limited access to information gathering functionality only. Tools capable of system modification are not available to regular Support Tools users.

This can be either a local group you define on the Support Tools Server machine or a domain group you define using Active Directory. During the Support Tools Server installation, you are prompted to enter the name of one (and only one) Windows user group that will serve as the Support Tools privileged group. Users in all other groups are treated as regular Support Tools users.

Using the Dashboard for the First Time

This topic describes some basic, important information on using the Support Tools Dashboard that all new users should be aware of.

Accessing Utilities in the Dashboard

All Support Tools utilities are accessed from the Support Tools menu. The menu groups utilities (with the exception of System Management which appears right under the main Support Tools heading) as:

- Interactive Mode

  – Select System

1)   The default support tools HTTP port is 8188.

- System Interrogate

- Registry

- Registry Compare

- Processes

- Services

- Trace and Log

- Common Tools (Including; Cisco and Third Party tools)

- Batch Mode

  - System Interrogate

  - Registry

  - Processes

  - Services

  - Trace and Log

  - Common Tools (Including; Cisco and Third Party tools)

Note that if you are not a member of the privileged user group, certain utilities will not be available to you and will not appear on the Support Tools menu. See About the Support Tools Utilities for a list of these privileged tools.

Selecting a System to Work With in Interactive Mode

The first action you typically take after logging in to the Dashboard is to select the system that you want to work with. Many Support Tools **Interactive Mode** utilities cannot be used until you first select a system.

Select the current system using the Select System utility. After you have completed working with that node, you can use the Select System utility to choose a different system to work with.

Adding a System to the System List

In order to select a system to work with, you may first need to add it to the Support Tools system list (if it is not already defined in the list). You can do this using the Select System or System Management screens.

You add multiple systems by clicking `Support Tools > System Management`.

In order to add a system to the list:

1. The Support Tools node must have been installed on the node, and

2. You must know the node's DNS entry or IP address.

Automated Node Addition: For CVP 4.x nodes and other Support Tools Servers the System Management page allows automated addition of CVP 4.x nodes and other Support Tools Servers.

Navigating and Refreshing Pages in the Dashboard

When using the Dashboard, it's important to navigate and refresh pages using only the controls in the Dashboard interface.

Avoid navigating and refreshing using controls belonging to your browser, specifically the browser Forward, Back, and Refresh commands. Dashboard pages expire as soon as a request for a subsequent page is made; therefore, using the browser's Forward and Back commands may return you to an expired page. Because the Dashboard uses a frameset, its pages may not refresh properly using the browser Refresh command.

How to Access the Support Tools Dashboard

To access the Support Tools Dashboard:

Step 1   Open a supported Web browser and in the Address line, enter (for example): `http://`
`<hostname>:8188/`.

Note: You can also specify the machine's IP address in place of its DNS entry. Note that the URL above uses Support Tools's default HTTP port.

Step 2   Press <Enter>. The Support Tools Dashboard Login screen opens.

Note: The default mode for Support Tools is to use SSL. You may see a warning such as the one pictured below. Click **OK** to accept the security certificate.

Figure 3: Login Security Warning
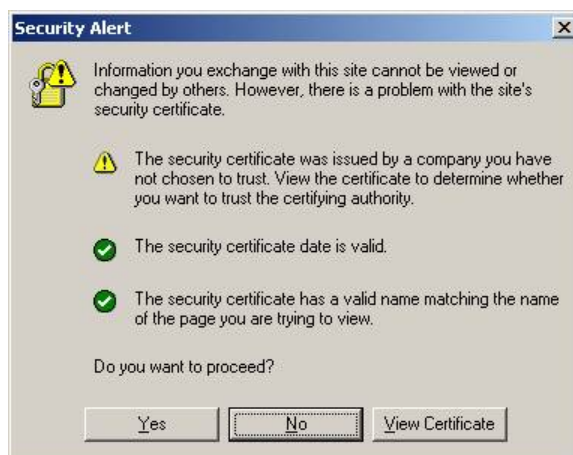
Step 3 In the Login Name field, enter `<Windows_domain>\<Windows_username>`. For example, `my_domain\my_username`.

Step 4 In the Password field, enter your Windows password (case-sensitive)

Step 5 Click Login.

How to Use the System Management Screen

Use the System Management screen to:

- Add Support Tools nodes to the Support Tools system list

- Remove nodes from the system list

- Test the connection between the Support Tools Server and a node

To open the System Management screen, from the Dashboard menu, select System Management.

To Add a Node to the System List

Adding a node to the system list makes it available for quick selection during future Dashboard sessions.

Step 1 In the Add Systems box, add the DNS entry or IP address of one or more Support Tools nodes.

Add each node on a separate line. Do not use a delimiter (for example, a comma) to separate entries.

Note: System host name can not be greater than 30 characters. Use the system's IP address if the host name is longer than 30 characters.

Note that entries are not validated for correctness.

Step 2   Click the Add System Button.

To Automatically Add CVP and Support Tools Server Nodes

Once you have added a CVP 4.x node or a Support Tools Server 2.1 node, you can automatically add all nodes defined on their system lists to the current Support Tools Server's system list.

Step 1   Add at least one CVP node and/or Support Tools Server node, following the process described in To Add a Node to the System List.

Step 2   In the System Management box, select the node you added.

Step 3   Check the Add Systems List from Tested Systems check box.

Step 4   Click the Test Connection button. Any new nodes are automatically added to the system list.

To Test the Connection to a Node

Testing the connection tests the connection between the Support Tools Server and one or more nodes.

Step 1   In the System Management box, highlight the Support Tools node(s) that you want to test.

Step 2   Click the Test Connection button.

If the system you attempt to test is not available, an error message displays. Check that: the node's DNS or IP address was entered correctly in the system list; the network connection to the node is active; the Support Tools Node Agent Service is installed and running on the node.

To Delete a Node from the System List

To delete a Support Tools node from the system list:

Step 1   In the System Management box, highlight the Support Tools node(s) that you want to delete from the list.

Step 2   Click the Remove Systems(s) button.

Using the Select System Screen

Selecting a system specifies the Support Tools node that you want to work with. You must select an ICM or related Cisco product node before you can interact with it through the Interactive Mode of the Support Tools Dashboard.

Note: Selecting a system is only required when you want to use **Interactive Mode** utilities. You do not need to select a system using the Select System screen when using **Batch Mode** utilities.

To open the Select System screen, from the Dashboard menu, select Interactive Mode > Select System.

Using the Select System Screen

To us the Select System Screen:

Step 1 To select a system from the existing System list, click the Select System radio button, and then highlight the system you want, OR...

To select a system not on the System list, click the Enter System Name radio button, and then enter the DNS entry or IP address for that node. Optionally, to also add this node to the System list, check Add To List Of Systems.

Step 2 Click Select System. The node is thereafter displayed as the current system at the top of each Dashboard Screen. Also indicated are the ICM product type(s) installed on the system.

These can include:

- ICM (AWs, PGs, Call Routers, and Loggers)

- Call Manager (CCM)

- CTIOS Server

- IPCC Express (CRS)

- Cisco Agent Desktop (CAD)

- Cisco Security Agent (CSA)

- Cisco Voice Portal (CVP)

- E-Mail Manager (CEM)

- Media Blender (CMB)

- Collaboration Server (CCS)

Note:

- This list may not be complete or accurate depending on your deployment. Node types are defined in a static configuration file and may differ from the ones listed here.

- If the system you attempt to select is not available, an error message displays. Check that: the node's DNS or IP address was entered correctly; the network connection to the node is active; the Support Tools Node Agent Service is installed and running on the node. If you are using the node's host name, try connecting to the host using its IP Address or fully qualified domain name instead.

Adding a Support Tools Node to the System List

Adding a node to the system list makes it available for quick selection during future Dashboard sessions. Adding a node to the system list also specifies it as the current system.

Step 1   Click Support Tools > Interactive Mode > Select System

Step 2   Click the Enter System Name radio button, and then enter the DNS entry or IP address for that node.

Step 3   Check Add To List Of Systems.

Step 4   Click Select System. The node is displayed as the current system at the top of the screen.

Note:

- If the system you attempt to select is not available, an error message displays. Check that: the node's DNS was entered correctly; the network connection to the node is active; the Support Tools Node Agent Service is installed and running on the node.

- To add multiple nodes more quickly, use the System Management Screen.

How to End a Dashboard Session

To terminate a Dashboard session, click the Logout link in the Dashboard. Dashboard sessions also time out automatically after 60 minutes after you close your browser.

Note:

- Sessions will time out when your browser remains open and no activity takes place for extended periods of time.

- Terminating a session will not terminate any Dashboard processes that may be running (for example, log collection). These will continue to run to completion.

- The Dashboard does not place a restriction on multiple logons. It is not necessary to terminate a session in order to begin a new one.

How to End a Dashboard Session

Part 5: Using Support Tools Web Tools

Support Tools Web Tools are a set of Cisco-authored utilities specifically designed for use with the Support Tools. They are installed on all Support Tools nodes.

Many Web Tools can be run either from the Support Tools Dashboard or via command line on an individual node. Command-line access to individual nodes can be local or remote (via methods like TelNet, pcAnywhere, etc.). However, they were primarily designed for Web access through the Dashboard.

All Web Tools allow you to save (to the Repository) and download file images of the data they collect.

Note: Within the Dashboard, the functionality of some Web Tools is distributed among several different screens (pages). For example, Processes and Services utility functionality is divided among a Processes screen and a Services screen.

Table 2: Web Tools at a Glance

Tool Name:	Description:	Installed On:	Dashboard Privileged Users Only:
Trace and Log	Use to collect and view log files from ICM or related Cisco Unified Product Nodes. Allows you to create merged logs from two ICM or related Cisco Product Nodes for comparative analysis, Also allows you to create trace groups for log groups, and turn on/off the different trace groups on a schedules basis.	All Support Tools nodes	
Registry	Use to view ICM or related Cisco Product Node registry entries.	All Windows-based Support Tools nodes	X
Registry Compare	Use to compare and synchronize Support Tools node registry entries	All Windows-based Support Tools nodes	X
System Interrogate	Use to display system information (for example, OS, hardware, ICM, SQL).	All Windows-based Support Tools nodes	
Processes	Use to view and stop Processes running on a Support Tools node.	All Windows-based Support Tools nodes	X
Services	Use to view and stop Services running on a Support Tools node.	All Windows-based Support Tools nodes	X

Chapter 11

Using Support Tools Utilities from the Dashboard

This section contains the following topics:

How to Use the System Interrogate Screen

Use the System Interrogate screen to view information about the current system.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For additional details on scheduling this tool to run in batch mode see Using Batch Mode (page 39). See below for details between the different options available in Interactive Mode and Batch Mode for System Interrogate.

Using System Interrogate you can:

- View system information on following:

    - Operating system and hardware

    - Cisco MCS Server

    - SQL Server Information

    - Web Server Information

    - Cisco JTAPI Information

    - ODBC Information

    - Cisco Security Templates

    - ICM 5.x 6.x or 7.x node

    - Cisco Callmanager (CCM)

    - Cisco Webview

    - Cisco SNMP

    - Cisco IPCC Express (CRS)

    - Cisco Agent Desktop (CAD)

    - Cisco Security Agent (CSA)

    Note: This is only a small subset of the list of information that you can view. The type of system information that can be retrieved depends upon the node type of the selected system. All of the above categories are not present for every node.

- After Interrogating the system you can save the data to a file.

There are differences between the type of information that System Interrogate can retrieve depending on whether it is running in Batch Mode or Interactive Mode.

In Batch Mode there is a fixed set of information that can be retrieved once selected for retrieval. This information includes:

- OS

- CPU

- Memory

- Disk

- Windows Hotfix

- Windows Domain

- Web Server (if present)

In Interactive Mode, the selected system is queried to determine which types of information are available for retrieval. This information includes the type of information that can be retrieved in batch mode and adds some additional types of information. See the table below for complete details.

Table 3: Types of Information Retrieved from System Interrogate

Component & Sub-components	Retrievable only in Interactive Mode
Windows OS • OS and Hardware Information • OS and Hardware Information (additional) • Dr. Watson Log File	
Cisco MCS • OS Image • OS Upgrade • OS Info • MSC Installation log files	X
Cisco Patches • Cisco Application Patches	X

Component & Sub-components	Retrievable only in Interactive Mode
SQL Server Information • SQL Server Registry Values • SQL Server WMI Values	
IIS Web Server • IIS Web Server	
Cisco JTAPI Information • Cisco JTAPI	
ODBC Information • ODBC	
Cisco Security Templates • Security Hardening Settings • Security Hardening Sections	
Cisco ICM 5.x, 6.x, or 7.x • ICM 5.x, 6.x, or 7.x	X
Cisco ICM 4.6.2 • ICM 4.6.2	X
Cisco IPCC Enterprise Web Administration • Client Properties File • Properties.xml file • Cisco CCBU Support Tools HTTP Server (Tomcat) log files • WebConfig log files	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco ICM/IPCC Agent Reskilling • Client Properties File • Properties.xml file • Cisco CCBU Support Tools HTTP Server (Tomcat) log files • WebConfig log files	X
Cisco WebView • Jaguar log files • ServletExec log files	X
Cisco SNMP • Content Center SubAgent log files • Management Service log files • Management Server Instance log files • Contact Center Trap Agent log files • Native SubAgent Adapter log files • Master Agent log files	
Cisco CTIOS Server 5.x • CTI Driver log files • CTI OS log files • NM log files • NMM log files	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco CTIOS Server 6.x • CTI Driver log files • CTI OS log files • NM log files • NMM log files	X
Cisco CTIOS Server 7.x • CTI Driver log files • CTI OS log files • NM log files • NMM log files	X
Cisco E-Mail Manager 5.x • CEM 5.x Registry Settings • Setup log files • WLCore log files	X
Cisco E-Mail Manager 5.x UI Server • CEM 5.x UI Server Registry	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco Agent Desktop (CAD) • CAD Registry Settings (Base) • CAD Registry Settings (Chat Server) • CAD Registry Settings (Directory Services) • CAD Registry Settings (Enterprise Server) • CAD Registry Settings (Framework) • CAD Registry Settings (IPPA) • CAD Registry Settings (LRM Server) • CAD Registry Settings (RASCAL Server) • CAD Registry Settings (Record and Playback Server) • CAD Registry Settings (Sync Server) • CAD Registry Settings (VoIP Monitor Server) • CAD Registry Settings (CAD Log files) • CAD Registry Settings (CAD Debug files)	X
Cisco CallManager 3.x • Build Information • Registry Information • CallManager Attendant Log files • CallManager Attendant Service log files • CallManager Attendant JTAPI log files • CallManager Installation log files	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco CallManager 4.x • Build Information • Registry Information • CallManager Attendant Log files • CallManager Attendant Service log files • CallManager Attendant JTAPI log files • CallManager Installation log files	X
Cisco Media Blender • CMB Properties files • CMB Blender Properties files	X
Cisco Collaboration Server • Registry Information • Current ccServer Err File • All ccServer Err files	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco IPCC Express • MSI Installer files • Node Manager EMS Files • Database ADS/HDS/RDS ReplLogs files • CRS SQL Server Logs • Editor Logs • Archive Tool logs • Alarm Server logs • Alarm logs • SNMP SYSAPP logs • SNMP CDP logs • Spanlink Agent/Supervisor logs • Spanlink Agent/Supervisor dbgs • Spanlink Install Manager files • Spanlink InstallShield silent install files • Spanlink InstallShield Install/Uninstall debug files	X
Cisco Voice Portal Application Server (all versions) • Registry Values • Installation log files	X
Cisco Voice Portal Application Server (2.x only) • AlarmForwarder EMS log files • ApplicationServer nm and nmm EMS log files • ApplicationServer properties files	X

Component & Sub-components	Retrievable only in Interactive Mode
Cisco Voice Portal Voice Browser (2.x only) • VoiceBrowser EMS log files	X
Cisco Contact Center Management Portal • Gateway Registry values • Provisioning Registry values • Provisioning InstallLog files • Provisioning InstallState files • Application Server Log files	X
Cisco Voice Portal SDDSN (2.x only) • Registry values • Installation log file	X
Cisco Voice Portal VXML Server (3.x only) • CVP VXML Installation log file • CVP VXML Server configuration files • CVP VXML Server log files • CVP VXML Application Server log files	X
Cisco Security Agent • Registry Values • csalog files	

Component & Sub-components	Retrievable only in Interactive Mode
Cisco Support Tools • Support Tools Version • Support Tools Server Settings • AppServer Log files • Command History files • Cisco CCBU Support Tools HTTP Server (Tomcat) log files • UIServer log files • UIServer WEB-INF UIRoot log files • Minidump files	X

Note: Service Releases and configuration changes may change the type of information that can be retrieved. The list above may not be complete or accurate for your deployment.

To Retrieve System Information in Interactive Mode

To retrieve system information for the current system:

Step 1 Verify that the system for which you want to interrogate is selected in the Interactive Mode > Select System screen.

Step 2 Click, Interactive Mode > System Interrogate.

Step 3 Select the options on which you want to retrieve data from the list of categories that appears. Only checked items will be interrogated.

Note: The types of options available differ depending on the type of system selected.

Step 4 Click System Interrogate.

Data is returned that corresponds to the options you have checked.

See below for information on saving the data collected.

To Retrieve System Information in Batch Mode

To retrieve system information in Batch Mode, From Support Tools > Batch Mode > System Interrogate:

Step 1   Select the Schedule Time to run the system interrogation. Select the Hours, Minutes, Month, Day, and Year.

Step 2   Select the system(s) that you want to interrogate by checking the box next the system name.

Step 3   Click Schedule. a Confirmation Screen Displays.

Step 4   Click OK.

You can view pending job by clicking on Support tools > Batch Mode> System Interrogate > Pending Jobs.

You can view completed interrogations by clicking on Support Tools > Batch Mode > System Interrogate > History.

To Save System Information to a File

As desired, you can save current system information to a file in the Support Tools Repository (for example, as a backup before editing).

To save system information to a file:

Step 1   Follow the steps above to interrogate the system.

Step 2   After the data appears, Click the Save button. A Save dialog box opens, displaying a default name for the file (`Sysquery_<Hostname>_<Datetime>.xml`).

Step 3   Accept the default name or enter an alternate.

> **Note:**
>
> • Files can only be saved to the Repository. Entering a path while saving has no effect.
>
> • All files are saved to an XML-formatted text file. While you can enter any extension you like, this will not affect the format in which the file is saved.

Step 4   Click OK. The file is saved to the Repository on the Support Tools Server.

Subsequent to saving, you can view or download saved files by selecting `Interactive Mode > System interrogate > History` from the Dashboard menu.

To Save Files Returned from a System Interrogate

Some interrogations retrieve files, such as log files, from the selected systems. You must specify that System Interrogate collect these files (such as selecting AppServer logs from a Support Tools Server)These files can be downloaded to your local system.

To download files returned from a system interrogate:

Step 1	Retrieve the information as noted above and view the resulting System Interrogate.
Step 2	Scroll down until you see a section containing a **Download** button. The download button signifies that the log file can be downloaded.
Step 3	Click **Download**. A pop-up dialog appears providing a link to download the file.
Step 4	Right-Click the link to download link and choose **Save as...** to download the file (typically a .zip file).
Step 5	Save the file to your local system.
Step 6	Click **Close** in the pop-up dialog box to close the window.

How to Use the History Screens

Use the History screens to work with Support Tools files previously saved to the Support Tools Repository.

You can; Set an Expiration Date, Download, View, Rename, and Delete Saved files.

You can access the following saved file types through the screen:

- System Interrogate files

- Registry files

- Registry Comparison files

- Process files

- Services files

To open the Files screen, from the Dashboard menu, select Support Tools **>** *<mode>* **>** *<tool>* **>** Files. The Files screen automatically displays all of the files of that type currently stored in the Repository.

Note: This utility is available to privileged users only. It will not appear on the Dashboard menu for non-privileged users with the following exception: non-privileged users can view System Interrogate files.

To Set an Expiration Date for History Files

All history files are automatically assigned an expiration date to conserve space and reduce file clutter. You toggle whether a file can expire or not by using te following steps:

Step 1   Check the Select box(es) of the file(s) that you can to expire/keep. If there is a date in the **Expires** column, then the file will be set to **No Expiration**. If it says **No Expiration** in the **Expires** field, then the file will be given an expiration date.

Step 2   Click **Keep/Expire**.

To View a Saved File

To view a saved file:

Step 1   Check the file's Select check box that you want to view.

Step 2   Click the View button. The contents of the file displays.

Step 3   To return to the file list, on the Dashboard menu, click the **Back** button.

To View Diff Only for Registry Compare Files (Registry Compare - History Screen Only)

To View only the differences in a saved Registry Compare File:

Step 1   Check the file's Select check box that you want to view.

Step 2   Click the View Diff Only button. The contents of the file displays, showing only differences in the saved registry compare file.

Step 3   To return to the file list, on the Dashboard menu, click the **Back** button.

To Rename a File

To rename a saved file:

Step 1   Check the file's Select check box.

Step 2   Click the Rename button. A Save dialog opens, displaying the current name of the file.

Step 3   Modify the name as desired. Note that all files are saved to an XML-formatted text file. While you can enter any extension you like, this will not affect the format in which the file is saved.

To Delete a File

To delete a file from the Repository:

Step 1   Check one or more of the file's Select check boxes.

Step 2   Click the Delete button.

Step 3   Click **OK** in the delete confirmation box.

To Download a File

As desired, you can download a copy of a file from the Repository to your local computer.

To download a file from the Repository:

Step 1   Check the file's Select check box.

Step 2   Click the Download button. A popup window opens containing two links: Download Text and Download XML.

Step 3   To download a file:

Depending on the type of file that you want to download:

- As plain text with no XML formatting, right-click the Download Text link and select Save Target As from the popup menu. A Save As dialog box opens.

- With any XML formatting intact, right-click the Download XML link and select Save Target As from the popup menu. A Save As dialog box opens.

Step 4   Specify the location where you want to save the download.

Step 5   Click Save.

How to Use the Registry Screen

The Registry Screen allows you to view a collapsible tree of the selected system's Windows registry.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see .

To use the Registry Screen

Step 1   Verify that the system for which you want to view the registry is selected in the Interactive Mode > Select System screen.

Step 2   Click **Get Registry**

The registry is shown in the left column. Clicking on the various nodes of this registry tree displays the node values in the right pane of the Registry Screen.

Step 3   You can optionally save the registry by clicking **Save**.

You can view saved registries by selecting `Interactive Mode > Registry > History`.

How to Use the Registry Compare Screen

Note: This tool can only be used in both **Interactive Mode**.

Use the Compare Registries screen to:

- Compare the Windows registry settings between:

  – The current system and another system

  – The current system and a registry file stored in the Support Tools repository

  – Two registry files in the repository

- Copy values from one system to another, or from a file to the current system

- Save a comparison to a file in the Repository

Support Tools has the ability to show only differences between registries. To see only differences between two systems, simply check the box for **Show differences only**.

To open the Compare Registries screen, from the Dashboard menu, select `Interactive Mode > Registry Compare`.

Note: This utility is available to privileged users only. It will not appear on the Dashboard menu for non-privileged users.

To Compare the Current System to Another

To compare registry settings from the current system to those of another system:

Step 1   Select the Compare to Another System radio button.

Step 2   Optionally select **Show differences only**. If selected, only differences between the two registries are displayed.

Step 3   Click the Compare Registries button. The systems list displays, showing all nodes defined in Support Tools.

Step 4   Highlight the system you want to use.

Step 5   Click the Compare Registries button.

To Compare the Current System to a Saved Registry File

To compare registry settings from the current system to those of a registry file previously saved in the Support Tools Repository:

Step 1   Select the Compare to Saved Registry File radio button.

Step 2   Optionally select **Show differences only**. If selected, only differences between the two registries is displayed.

Step 3   Click the Compare Registries button. A list of registry files saved in the Repository displays.

Step 4   Select the file you want to compare to.

Step 5   Click the Registry Compare to File button.

To Compare Two Saved Registry Files

To compare the contents of registry settings from two registry files previously saved to the Support Tools Repository:

Step 1   Select the Compare Two Saved Registry Files radio button.

Step 2   Optionally select **Show differences only**. If selected, only differences between the two registries is displayed.

Step 3   Click the Compare Registries button. A list of registry files saved in the Repository displays.

Step 4   Select the files you want to compare.

Step 5   Click the Compare Registries Files button.

Understanding the Compare Registries Display

Once you have selected the systems or files you want to compare, the Compare Registries screen displays the comparison in a three-pane view as shown in this example:

Figure 4: Compare Registries Display
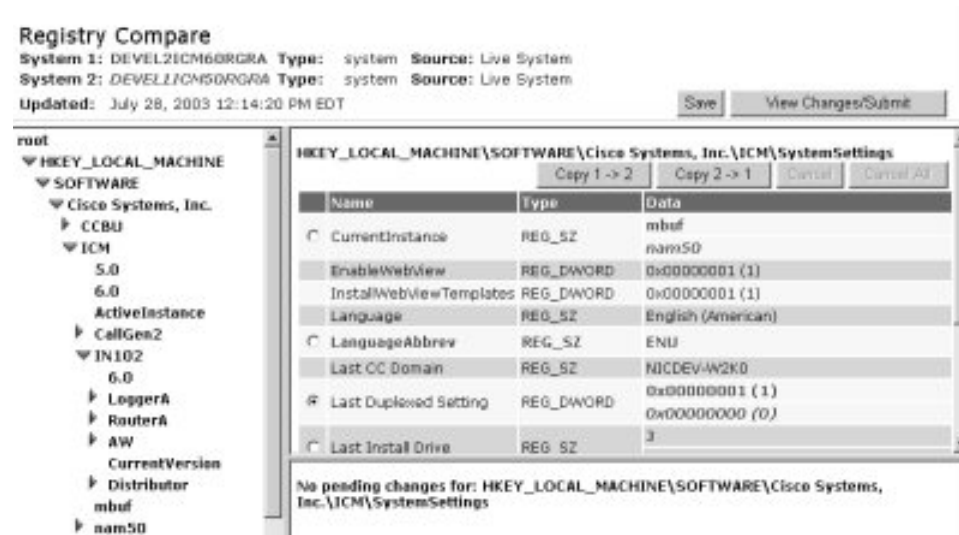
The Display shows the following:

- The top pane shows the systems or files being compared. System 1, the current system or first file being compared, is color-coded in brown bold. System 2 is color-coded in green italic bold.

- The left-hand pane shows a tree view of keys which includes keys from both systems.

- The right-hand pane shows (at the top) the path for the selected key, and (beneath) values for that key. Each value is composed of three parts: a name, a type, and data. These are color coded as follows:

  - Parts of a value are identical on both systems are shown in black normal font.

    Note: If you selected **Show differences only** then parts that are identical are not displayed, however if the results are saved it is still possible to view the complete registry at a later time.

  - Parts of a value that exist only on System 1 are shown in brown bold.

  - Parts of a value that exist only on System 2 are shown in green italic bold.

Note: For information on how to copy key values from one system to another, see To Copy Keys Between Registries and Files below.

Viewing Registry Keys for Multiple Customer Instances

For machines with multiple customer instances, the Compare Registries screen only retrieves and displays the registry settings for one instance at a time. By default, the screen retrieves the registry for the first customer instance it encounters on each machine based on an alphabetical listing of instance names. (The currently loaded instance will display an arrow to the left of its name, indicating content.)

To retrieve the registry for a different instance.

Step 1   In the registry tree, navigate to and expand the ICM branch. All customer instances are displayed. The currently loaded instance will display an arrow to the left of its name, indicating content.

Step 2   Click the name of the instance whose registry you want to retrieve. A message displays stating: "Insufficient data available for comparison."

Step 3   Click the Compare Registries Again link to retrieve registry data for that instance.

To Copy Key Values Between Registries and Files

After initiating a registry comparison, you can copy specific key values from one system to another in order to synchronize similar systems, or to correct missing or incorrect values on a system.

You can copy key values from one system to another, or from a file to the current system. Note that you cannot copy values between files, or from a system to a file.

Warning: Incorrect modification of registry settings can have serious consequences. Do not change ICM registry settings unless it is absolutely necessary and you are fully aware of the ramifications. It is strongly advised that you first save a registry comparison to a file before making changes.

To copy registry key values:

Step 1   With a comparison displayed, navigate the registry tree to the key whose value you want to copy.

Step 2   Select the value by clicking its radio button. Values whose data cannot be copied (for example, because the values are already identical, or because you are comparing two files) will not have a radio button.

Note: For an explanation of key value color-coding, see Understanding the Compare Registries Display above.

Step 3   Click the appropriate Copy button (Copy 1 > 2 or Copy 2 >1) to indicate the direction in which the value should be copied. If you are comparing a system to a file, you can only copy to the system.

Step 4   Continue selecting additional values, as desired. Values selected for copying are listed in the lower-right portion of the screen.

As necessary, to undo:

- The most recent selection, click the Cancel button

- All selections, click the Cancel All button

Step 5   To proceed with changes, click the View Changes/Submit button. All pending changes are listed.

Step 6   Click Submit to finalize your changes.

To Save a Registry Comparison to a File

As desired, you can save a registry comparison to a file in the Support Tools repository for future study or reference. Saving saves the complete retrieved Cisco branch of both registry trees--not just the currently expanded portion of that branch.

Note that in the case of machines with multiple customer instances, only values from the currently retrieved instances are included in the file.

To save a registry comparison to a file:

Step 1   Click the Save button. A Save dialog box opens, displaying a default name for the file (`RegCompare_<system1>_<system2>_<Datetime>.xml`).

Step 2   Accept the default name or enter an alternate.

Note:

- Files can only be saved to the Repository. Entering a path while saving has no effect.

- All files are saved to an XML-formatted text file. While you can enter any extension you like, this will not affect the format in which the file is saved.

Step 3   Click OK. The file is saved to the Repository on the Support Tools Server.

Note: Subsequent to saving, you can view or download saved files by selecting Compare Registries > Files from the Dashboard menu.

How to Use the Processes Screen

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see Using Batch Mode (page 39).

Use the Processes screen to:

- View all processes running on the current system

- Terminate processes on the current system

- Save a list of processes to a file

To open the Processes screen, from the Dashboard menu, select Support Tools **>** *<mode>* **>** Processes.

Note: This utility is available to privileged users only. It will not appear on the Dashboard menu for non-privileged users.

To View Processes

To view processes for the current system:

Step 1   Click the View Processes button. The screen displays all processes currently running on the system.

For each process, the screen displays:

- Name: The name of the process.

- PID: The process's ID number.

- Type: Either Critical (blue), Known, (green), or unknown (red). This categorization for each process is based on modifiable process definitions stored in the Processes Definition List.

- Information: Additional information about the process as defined in the Processes Definition List.

Note: Support Tools automatically downloads the list of current processes at the time you connect to a system. If you suspect the system's processes have changed since you first connected to it, click the Refresh button to refresh the list.

To Save a Process

To terminate a process on the current system:

Step 1   Click the Save button. A Save dialog box opens, displaying a default name for the file (<Listtype><Hostname><Datetime>.xml).

Step 2   Accept the default name or enter an alternate.

Note:

- Files can only be saved to the Repository. Entering a path while saving has no effect.

- All files are saved to an XML-formatted text file. While you can enter any extension you like, this will not affect the format in which the file is saved.

Step 3   Click OK. The file is saved to the Repository on the Support Tools Server.

Step 4   Subsequent to saving, you can view or download saved files by selecting Processes > Files from the Dashboard menu.

To Terminate a Process

To terminate a process on the current system:

Step 1   Select a checkbox next to the process(es) that you want to terminate.

Step 2   Click Terminate. a Confirmation Page appears showing the process(es) that you selected to terminate.

Step 3   Click Terminate to terminate the process, or cancel to not terminate the process(es).

How to Use the Services Screen

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see Using Batch Mode (page 39).

Use the Services screen to:

- View all Services installed on the current system

- Stop and start services on the current system

- Save a list of Services to a file

To open the Services screen, from the Dashboard menu, select Support Tools > <mode> Services.

Note: This utility is available to privileged users only. It will not appear on the Dashboard menu for non-privileged users.

To View Services

To view services for the current system:

Step 1   Click the List Services button. The screen displays all services on the system.

For each service, the screen displays:

- A check box whose column (Start/Stop) indicates whether the service is currently running.

- Name: The name of the service.

- Type: Either Critical (blue), Known, (green), or unknown (red). (Service type is defined in the user-modifiable **processinfo.xml** file.)

- Information: Additional information about the service as defined in the Services Definition List.

Note: Support Tools automatically determines the state of current services (started or stopped) at the time you connect to a system. If you suspect these states have changed since you first connected to the system, click the Refresh button to refresh the list.

To Stop or Start a Service

To stop or start a service on the current system:

Step 1   With the list of services displayed, select the appropriate check box (Start or Stop) for one or more services.

Note: You cannot stop Critical (blue) services. Critical services are those that your company has designated as essential to the health of the current system. For these services, the Select/Stop check box is disabled.

Step 2   Click the Start/Stop Services button. A confirmation screen displays, listing the services selected for an action.

Step 3   Click the Start/Stop Services button.

Note:

- Prior to stopping a service, you should be aware of the significance of stopping it, including any dependant services that may be affected. Note that the Cisco CCBU Support Tools Node

Agent Service is required for the Support Tools Server to maintain a connection with the current system. Stopping this service will terminate your connection.

- The Services screen will not allow you to stop services with peer or child dependencies while those dependencies are running. If you attempt to stop such a service, the Dashboard returns a message alerting you that dependencies exist.

To Save the Services List to a File

As desired, you can save a system's Services list to a file in the Support Tools repository. These files can later be viewed or downloaded locally using the Files screen.

To save Services to a file:

Step 1   Click the Save button. A Save dialog box opens, displaying a default name for the file (Services<Hostname><Datetime>.xml).

Step 2   Accept the default name or enter an alternate.

Note:

- Files can only be saved to the Repository. Entering a path while saving has no effect.

- All files are saved to an XML-formatted text file. While you can enter any extension you like, this will not affect the format in which the file is saved.

Step 3   Click OK. The file is saved to the Repository on the Support Tools Server.

Step 4   Subsequent to saving, you can view or download saved files by selecting Services > Files from the Dashboard menu.

Trace and Log

Trace and Log tools allow you to collect logs from systems that have Cisco products installed. Trace and Log tools can be used in either Interactive Mode (for the current system) or Batch mode (for multiple systems).

Log groups define which products and process should be queried to retrieve logs. Logs can be merged to provide a consolidated time-sorted view.

Trace groups define trace level settings that are associated to the products and processes defined in a log group. You can set trace groups to activate and deactivate over a period of time. Collected logs reflect the trace settings that were active for the period of time specified when the log collection was requested. This configuration allows for great flexibility in logging. You can, for instance, collect logs for a Log group at a default trace setting, then activate a trace group to change the trace settings and collect the logs again, and revert to the default trace (or another trace group) after the logs have been collected using the new trace settings.

Trace and Log: Interactive Mode

Interactive Mode Trace and Log allows you to set trace levels and collect logs against the currently selected system. It includes these tools:

- Set Trace

- Collect Logs

You access Interactive Mode Trace and Log tools by selecting **Interactive Mode > Trace and Log**.

Trace and Log: Batch Mode

Batch Mode Trace and Log allows you to set trace levels and collect logs against multiple systems. It includes these tools:

- Create Log Group

- Create Trace Groups

- Schedule Trace

- Collect Logs

You access Batch Mode Trace and Log tools by selecting **Batch Mode > Trace and Log**.

How to Use the Create Log Group Screen

Use the Create Log Group Screen to create a log group. A log group is a specification that defines the products, systems, and processes you want to pull logs for.

To open the Create Log Group screen, from the Dashboard menu, select Batch Mode > Trace and Log > Create Log Group.

To Create a Log Group

To create a log group:

Step 1   Select the Cisco product(s) whose logs will be collected by this group.

You can collect logs for:

- ICM (AWs, PGs, Call Routers, and Loggers)

- Call Manager

- Collaboration Server

- E-Mail Manager

- Media Blender

- IPCC Express

- Cisco Agent Desktop

- Cisco Voice Portal (Application Server, Voice Browser, Alarm Forwarder, and Audium logs. Log collection for Audium is supported for CVP 4.0 and above, only.)

Note: Cisco Security Agent (CSA) Logs cannot be downloaded using this tool. They are available as a download option during the interactive mode of System Interrogate.

Step 2   Click Next. All nodes defined on the Support Tools system list that belong to the selected products are listed.

Note: This list may also include any nodes whose product type is unknown (blank). The most common reason for an unknown product type is that the node has never been contacted by the Support Tools Server. For example, it was added to the system list (via System Management screen) but the connection was not tested or the node has never been selected as a current system. It is also possible that the ICM component was added or modified after the tool had already connect to the node.

Step 3   Select the system(s) whose logs you want to collect.

Step 4   Click Next.

Step 5   Enter a name (up to 32 characters long), and optionally a description, for the log group. It's a good idea to choose an intuitive name that will help other users understand what type of logs this group collects.

Step 6   Indicate which system processes you want to collect logs for. The available choices depend on which type of system has been selected.

- ICM Processes Logs:

    - System: The ICM system name

    - Customer: The ICM customer instance(s) on the system

    - Node: The ICM node ID (for example, pg1a, pg1b, router a, router b)

- Process: The process(es) on that node for which logs can be collected.

- CCM Process Logs:

  - System: The CCM system name

  - Node: The CCM process(es) for which logs can be collected--CCM or CTI.

- IPCC Express Process Logs:

  - System: The CRS system name

  - Node: The IPCC Express Node on the system

- CAD Process Logs:

  - System: The CAD system name

  - Process: The process(es) on that node for which logs can be collected.

  - Debug: Check to include debug information in the log.

- CSA Process Logs:

  - System: The CSA system name

- CVP Process Logs:

  - System: The CVP system name

  - Node: The CVP Node on the system

- CCS Process Logs:

  - System: The CCS system name

- CMB Process Logs:

  - System: The CMB system name

- CEM Process Logs:

  - System: The CEM system name

Step 7   If any of the systems you selected are unavailable for log collection (for example, if they are offline, a message will display on the screen alerting you to the fact.

Step 8   Click Finish. The log group is now available to use in a log collection (on the Collect Logs screen) or in a trace group (on the Create Trace Group screen).

How to Use the Log Groups Screen

The Log Groups screen displays defined log groups. From this screen you can View, Edit, Rename, and delete Log Groups.

Viewing Log Groups

You can view the details of any log group on the log group screen. To view a log group's details:

Step 1 From the History - Log Group screen, check the Select box next to the Log Group whose details you want to view.

Step 2 Click View

Step 3 The screen displays which products and processes have been selected for this log group.

Step 4 Optionally, click Edit to edit this log group. Follow the instructions below for **Editing Log Groups**.

Editing Log Groups

Editing a log group re-runs the Log Group creation wizard with the current settings for this existing log group preselected. To Edit a log group:

Warning: Do not modify Log Groups that have been used to create a Trace Group. This may cause unexpected results when using the trace tool to automatically collect logs.

Step 1 From the History - Log Group screen, check the Select box next to the Log Group whose details you want to edit.

Step 2 Click Edit.

Step 3 The Create Log Groups wizard is invoked with the current setting for this log group preselected.

Step 4 Change settings as required using the wizard as described in How to Use the Log Groups Screen (page 107).

Renaming Log Groups

You can change the name of any log group. To change a log group's name:

Warning: Do not rename Log Groups that have been used to create a Trace Groups. This may cause unexpected results when using the trace tool to aromatically collect logs.

Step 1   From the History - Log Group screen, check the Select box next to the Log Group whose name you want to change.

Step 2   Click Rename.

A dialog box appears prompting you for a new name.

Step 3   Enter the new name in the dialog box and click OK.

The name is instantly changed and the change is reflected in the History - Log Group screen.

Deleting Log Groups

To delete one or more log groups:

Step 1   From the History - Log Group screen, check the Select box(s) next to the Log Group(s) that you want to delete.

Step 2   Click Delete

A Confirmation Dialog Box appears.

Step 3   Click OK in the confirmation dialog box to delete the log group(s).

The log group(s) are instantly deleted and the results appear on the History - Log Group screen.

Refreshing the Log Groups Screen

You can refresh the view of log groups at any time. Refreshing the view allows you to see changes other uses may have made in the recent past.

Note: The screen is automatically refreshed each time it is loaded.

To refresh the list of log groups:

Step 1   From the History - Log Group screen, click Refresh.

Step 2   The screen is refreshed showing any updates that may have been made.

How to Use the Create Trace Group Screen (Batch Mode)

Trace Groups allow to set the trace level for products and precesses defined in a log group.

Creating a Trace Group

Note: Not all Cisco Unified components and processes are supported. When a component in a log group is not supported a specific message noting that the component is not supported displayed.

To Create a Trace Group:

Step 1   From the Create Trace group Screen, select a Log Group Name and click Next.

Trace Groups are based on the products and processes defined in a Log Group. You must first Create a Log Group (page 107) before you can create a Trace group.

Step 2   Enter a name (up to 32 characters long), and optionally a description, for the trace group. It's a good idea to choose an intuitive name that will help other users understand what type of logs this group collects.

Step 3   A List of configurable trace setting is displayed on the page for each trace tool that is available to set trace levels for the products and processes defined in the log group. For each section of trace settings you can choose **Low**, **Medium**, **High**, or **Current** trace setting for the section, or optionally select individual settings from within the section. Checking the Low, Medium, High, or Current will automatically check settings for that section based on predefined values.

Mousing over any of the setting check boxes may display a pop-up help box that describes the setting.

Note: The "Current" setting does not always display the actual current trace settings on the server.

Step 4   Click Finish when you have completed making your trace setting selections.

A confirmation page displays notifying you that the trace group has been created.

Step 5   Click OK to return to the Create Trace Group Screen.

How to Use the Create Trace Group Screen (Interactive Mode)

Trace Groups allow you to set the trace level for products and processes defined in a log group. In Interactive Mode, you set the trace level for the currently selected system.

To access the Create Trace Group screen in Interactive Mode, select Interactive Mode > Trace and Log > Set Trace.

Creating a Trace Group

Note: Not all Cisco Unified components and processes are supported. When a component in a log group is not supported a specific message noting that the component is not supported displayed.

To Create a Trace Group in Interactive Mode:

Step 1 From the Create Trace Group screen, click Get Trace Settings.

Trace Groups are based on the products and processes defined in a Log Group. You must first Create a Log Group (page 107) before you can create a Trace group.

Step 2 A List of configurable trace setting is displayed on the page for each trace tool that is available to set trace levels for the products and processes defined in the log group. For each section of trace settings you can choose **Low**, **Medium**, **High**, or **Current** trace setting for the section, or optionally select individual settings from within the section. Checking the Low, Medium, High, or Current will automatically check settings for that section based on predefined values.

Mousing over any of the setting check boxes may display a pop-up help box that describes the setting.

Note: The "Current" setting does not always display the actual current trace settings on the server.

Step 3 Click Finish when you have completed making your trace setting selections.

A confirmation page displays notifying you that the trace group has been created.

Step 4 Click OK to return to the Create Trace Group Screen.

How to Use the Trace Groups Screen

The Trace Groups Screen (History - Trace groups) allows you to View a trace group's settings, Edit the trace group's settings, Rename or delete the trace group, or refresh the list of trace groups.

Viewing a Trace Group's Settings

To view a Trace Group's Settings:

Step 1 From the History - Trace Group screen, check the Select box next to the Trace Group whose settings you want to view.

Step 2 Click View Settings

Selected settings for this Trace group Appear. The settings show the values **currently** set on the node. These settings are not the ones set for the Trace group. To view the values set in the trace group use the **View File** command.

Viewing a Trace Group's File

To view a Trace Group's File:

Step 1   From the History - Trace Group screen, check the Select box next to the Trace Group whose file you want to view.

Step 2   Click View File

Selected settings for this Trace group Appear.

Mousing over any of the setting check boxes may display a pop-up help box that describes the setting. The values shown are the settings defined for this trace group. Note that this differs from the **View Settings** command in that the View Settings command shows the values **currently** set for the node.

Step 3   You can optionally **Edit** the Trace Group File by clicking Edit.

Editing a Trace Group

To Edit a Trace Group"

Step 1   From the History - Trace Group screen, check the Select box next to the Trace Group that you want to edit.

Step 2   A List of configurable trace setting is displayed on the page for each trace tool that is available to set trace levels for the products and processes defined in the log group. For each section of trace settings you can choose **Low**, **Medium**, **High**, or **Current** trace setting for the section, or optionally select individual settings from within the section. Checking the Low, Medium, High, or Current will automatically check settings for that section based on predefined values.

Mousing over any of the setting check boxes displays a pop-up help box that describes the setting.

Note: The "Current" setting does not always display the actual current trace settings on the server.

Step 3   Click Finish when you have completed making your trace setting selections.

A confirmation page displays notifying you that the trace group has been created.

Step 4   Click OK to return to the Create Trace Group Screen.

Renaming Trace Groups

You can change the name of any trace group. To change a trace group's name:

Step 1   From the History - Trace Group screen, check the Select box next to the Trace Group whose name you want to change.

Step 2   Click Rename.

A dialog box appears prompting you for a new name.

Step 3   Enter the new name in the dialog box and click OK.

The name is instantly changed and the change is reflected in the History - Trace Group screen.

Deleting Trace Groups

To delete one or more Trace Groups:

Step 1   From the History -Trace Group screen, check the Select box(s) next to the Trace Group(s) that you want to delete.

Step 2   Click Delete

A Confirmation Dialog Box appears.

Step 3   Click OK in the confirmation dialog box to delete the Trace group(s).

The trace group(s) are instantly deleted and the results appear on the History - Trace Group screen.

Refreshing the Trace Groups Screen

You can refresh the view of trace groups at any time. Refreshing the view allows you to see changes other uses may have made in the recent past.

Note: The screen is automatically refreshed each time it is loaded.

To refresh the list of trace groups:

Step 1   From the History - Trace Group screen, click Refresh.

Step 2   The screen is refreshed showing any updates that may have been made.

How to Use the Schedule Trace Screen

The Schedule Trace screen allows you to define a period of time when a certain trace level setting should be used (as defined in a trace group) and optionally collect and merge logs, and collect binary data. Finally, you can define the trace level setting that the traces should revert to at the end time of the Schedule Trace period.

Scheduling a Trace

To schedule a trace, from the Schedule Trace Screen:

Step 1   Define a start time when the trace level in the selected trace group(s) should be activated. Select the Hour, Minute, Day, Month, and Year. You can click on the Days in the calendar.

Step 2   Define an end time when the trace level in the selected trace group(s) should be deactivated. Select the Hour, Minute, Day, Month, and Year.

Note: The End Time must occur after the start time.

Step 3   In the **At End Time** section,

Define the following:

- Optionally check the box next to **Restore trace level to:** and select either *Low* or a trace group

  to change or restore the trace level after the end time of the trace.

- Optionally check **Collect Logs** and provide a log collection name to collect the logs defined in the Log Group for this Trace Group.

- If you checked **Collect Logs:** you can optionally check **Merge Logs** to merge the logs collected during this trace.

- If you checked **Collect Logs:** you can optionally check **Include Binary Data** to include this data in the log collection.

Note: See How to Use the Collect Logs Screen (page 117) for details on Log Collection, Merged Logs, and Including Binary data.

Step 4   Select the Trace Group(s) that you want to activate during the defined period of time by checking the select box next to the Trace Group File Name.

Step 5   Click **Schedule Trace** to create the trace.

Step 6   A confirmation page appears. Click OK.

The Pending Jobs created can be seen in **Batch Mode > Trace and Log > Schedule Trace > Pending Jobs**.

About Log Collection

Use the Collect Logs Screen to collect logs from ICM or related Cisco product nodes running the Support Tools Node. Multiple collected logs can be retrieved as separate files or merged into a single file to provide a consolidated unified time-sorted view.

Products Supported for Log Collection

Support Tools allows you to collect logs for:

- ICM (AWs, PGs, Call Routers, and Loggers)

- Call Manager (CCM)

- Collaboration (CCS)

- Email-Manager (CEM)

- Media Blender (CMB)

- IPCC Express (CRS)

- Cisco Agent Desktop (CAD)

- Cisco Security Agent (CSA)

- Cisco Voice Portal (CVP)

Note: Log collection for CTIOS is not supported.

Collect Logs: General Steps

In order to collect logs in Support Tools you must:

Step 1 Create log groups: A log group defines the products, systems, and processes whose logs you want to collect. You must create a log group before you can begin collecting logs. You can create different log groups to target different products and systems.

Log group definitions are saved in the Support Tools Repository and are available for subsequent re-use by other Support Tools users. They can be modified or deleted as necessary.

Step 2 Create a log collection request: A log collection request defines the time range of logs to collect, what log groups to include in the request, and whether the logs should be merged into a single

file, or delivered as individual files. You define when you want the logs collected by specifying a start and end time.

Each log collection request can be run only once. The logs it collects are stored in the Repository where they remain until you choose to delete them (by deleting the log collection to which they belong). Collected logs can be downloaded locally for viewing.

What are Merged Logs?

The Collect Logs Screen allows you to create merged logs, logs which combine different logs from different systems into a single file. Within a merged log, individual log entries are listed by date and time, allowing you to track, for example, the routing of an individual call across different ICM systems.

There is no limit to the number of individual system logs that can be included in a single merged log file. Note however that larger logs will take longer to collect.

When you download a merged log collection, you can download both the individual associated logs in addition to the merged log itself.

Merged logs are subject to the following limitations:

- To use merged log capabilities, each Support Tools Server and node must be able to communicate with the same Simple Network Time Protocol (SNTP or NTP) server. If any system in a merged log collection cannot communicate with the SNTP server, the merge will fail, and the outputted log will contain the alert: "Missing SNTP data for all of the following files logs prevented merging logs:..."

- Some logs do not record time in milliseconds: Some logs record events up to the second, while others record seconds and milliseconds. The Merge logic assumes zeros when milliseconds are missing.

- Even with a properly configured SNTP server, there can be slight drift in time: Used in conjunction with a properly configured SNTP server, each Support Tools node tracks deviation between the system clock and the network standard clock. That difference is used to adjust each log entry. Since time is adjusted in increments of 8 minutes, minor millisecond differences can occur.

- Within a merged log, event ordering can be altered by OS pre-emotion: Within the same system, processes are pre-empted by the OS. It is possible for ordering in the log to be affected by OS preemption.

- A Merged Log Collection must span a time greater than the time server sample interval across all included nodes to be collected.

Log entries in merged logs are prefaced by the following identifiers:

Table 4: Viewing Entries in Merged Logs

ICM Log Entries	ICM @ <host_name> + <customer_instance>, <ICM_node>, <process>: (<utc date/time>) <local date/time>
CCM Log Entries	CCM @ <host_name> + <CCM_node>: (<utc date/time>) <local date/time>
CCS, CEM, and CMB Log Entries	<product> @ <host_name> +: (<utc date/time>) <local date/time>

For example, an ICM log entry might be prefaced by:

```
ICM@my_logger + instance_1, logger_a, ccag:(09/04/2006 18:30:00) 09/
04/2006 12:30:00
```

Note that in a merged log:

- UTC date/time represents the *adjusted* date/time of a log entry based on your network's SNTP server clock.

- Local date/time represents the *unadjusted* date/time of a log entry based on the clock of the system from which the log was derived.

How to Use the Collect Logs Screen (Batch Mode)

Use the Collect Logs Screen to create a log collection. A log collection is a specification that defines the log group(s) and time range you want to collect logs for.

To open the Collect Logs screen, from the Dashboard menu, select Batch Mode > Trace and Log > Collect Logs

Note: For information on the Merge Logs option see About Log Collection (page 117)

To Create a Log Collection

To create a log group:

Step 1   Enter a name (up to 32 characters long) for the log collection. It's a good idea to choose an intuitive name that conveys the attributes of the log collection.

Step 2   Optionally, enter a description up to 255 characters long.

Step 3   Use the calendar to specify the time range of logs to collect.

Step 4   Optionally, specify whether you want this log collection to run on a recurring frequency.

Step 5   Optionally, check Merged Log to create a single merged log file from the logs collected by this group.

Note: When you later download a merged log, the collection will include the individual associated log files in addition to the merged log itself.

Step 6   Optionally, for ICM system logs only, check Include Binary Data. This causes the log file to include binary data such as memory allocation, buffer size, etc., but may also substantially increase file size.

Step 7   Optionally, for ICM system logs only, check Use MS Option for Dumplog. This causes dump log files to include data in millisecond increments, but may also substantially increase file size.

Step 8   Optionally, for CVP 4.0+ logs only, check Collect Only Error Logs. This limits log collection to error logs.

Step 9   Select one or more log groups to collect logs from.

Step 10   Click the Start Log Collection button. The log collection process begins according to the times you specified. The amount of time this process takes to complete depends on the number and size of the logs you requested, as well as the period of the collection that you specified when you entered a start and end time. You can view collected logs or check the status of requests on the Log Collections screen.

Note: It is not necessary to remain in-session while a log collection runs. Exiting your Dashboard session will not terminate a log collection. You can proceed to use other Dashboard Utilities while a Log Collection runs.

How to Use the Log Collections Screen

Use the Log Collections Screen to view and administer collected logs. You can:

- View details of log collections

- Download collected logs

- Delete log collections

- Rename Log Collections

To open the Log Collections screen, from the Dashboard menu, select Batch Mode > Trace and Log > Collect Logs > Log Collection.

To View Details of Log Collections

The Log Collection screen automatically lists each collection currently stored in the Support Tools repository. For each collection, the screen displays:

- Name: The name of the collection.

- Description

- Requested: The date/time its request was sent.

- Log Period: The start and end time of the collection.

- Merge Logs: Whether or not this is a merged log collection.

- Binary Data: Whether or not binary data was included in the log.

- Log Groups: The log group used for this collection.

Additionally, the following information is available for each Node in which information was collected for this log collection:

Item	Description
System	The name of the system from which logs were collected.
Node	The component or node type from which logs were collected.
Log Collection - Log Group	The name of the Log Collection and the Log Group.
Status	The status of the request.
	Ready signifies that the log can be downloaded.
	In progress signifies that the log collection has not completed.
	Failed indicates that there was an error and the log collection attempt failed.

To Download Collected Logs

Collected logs can only be viewed after downloading to your local machine; they cannot be viewed from within Support Tools.

To download collected logs:

Step 1 Check the Select check box for the collection whose logs you want to view. You can only download the logs from one collection at a time. If necessary, before proceeding, verify that the collection's status is Ready (complete).

Step 2   Click the View button. Details of the collection, along with the individual log files it contains, are displayed. If the log collection included a merged log, both the individual associated log files and the merged log file are listed.

Step 3   Check the Select check box for the logs you want to download. If you select individual logs from a merged log collection, the merged log will automatically download along with the individual logs you select.

Step 4   Click the Download button.

Step 5   When prompted, choose the Save to Disk option.

Note: Logs download in a single zip file which must be extracted in order to view.

Log File Naming Conventions

Log files use the following naming conventions:

- For ICM:
  `<collection-group>{<product>{<NodeAgentHost>(<customer>,<node>,<process>.log`

- For CCM: `<collection-group>{<product>{<NodeAgentHost>(<node>.log`

- For other products: `<collection-group>{<product>{<NodeAgentHost>.log`

To Delete a Log Collection

To delete a log collection:

Step 1   Check the collection's Select check box.

Step 2   Click the Delete button.

Step 3   A message displays prompting you to confirm the deletion.

Step 4   Click OK.

To Rename a Log Collection

To Rename a log collection:

Step 1   Check the collection's Select check box.

Step 2   Click the Rename button.

Step 3 A Dialog Boc displays prompting you to enter a new name, enter the new name in the dialog box and click OK.

How to Use the Collect Logs Screen (Interactive Mode)

Use the Collect Logs Screen to create a log collection. A log collection is a specification that defines the log group(s) and time range you want to collect logs for. In Interactive Mode, you create log groups for the currently selected system.

To open the Collect Logs screen, from the Dashboard menu, select Interactive Mode > Trace and Log > Collect Logs.

To Create a Log Collection

To create a log collection:

Step 1 Optionally, check Merged Log to create a single merged log file from the logs collected by this group.

Note: When you later download a merged log, the collection will include the individual associated log files in addition to the merged log itself.

Step 2 Optionally, for ICM system logs only, check Include Binary Data. This causes the log file to include binary data such as memory allocation, buffer size, etc., but may also substantially increase file size.

Step 3 Optionally, for ICM system logs only, check Use MS Option for Dumplog. This causes dump log files to include data in millisecond increments, but may also substantially increase file size.

Step 4 Optionally, for CVP 4.0+ logs only, check Collect Only Error Logs. This limits log collection to error logs.

Step 5 Specify a time span (in minutes) of logs to collect.

Step 6 Select one or more log groups to collect logs from.

Step 7 Click the Collect LOGS button. The log collection process begins immediately. The amount of time this process takes to complete depends on the number and size of the logs you requested, as well as the period of the collection that you specified. You can view collected logs or check the status of requests on the Log Collections screen.

Note: It is not necessary to remain in-session while a log collection runs. Exiting your Dashboard session will not terminate a log collection. You can proceed to use other Dashboard Utilities while a Log Collection runs.

How to Use the Collect Logs Screen (Interactive Mode)

Chapter 12

Using Cisco Tools from a Command Line

While primarily designed for use through the Dashboard, Cisco Tools can also be run from a command line on any Support Tools node. This can be useful when access to the Support Tools Server/Dashboard is not available due to a down machine or connection.

The functionality available in the Dashboard versions of these utilities is similar, though not identical, to their command line counterparts. As GUIs are generally easier to learn, it is a good idea to familiarize yourself with these tools in the Dashboard before attempting to use them from a command line.

Note: The command line versions of the tools cannot download attachments that could normally be downloaded when using the web-based version of the tool. You must used the web-based version of the tool if you need to download attachments.

Command line versions of the utilities are installed and can be run from any Support Tools node. Their default location (modifiable during installation) is: *c:\cisco\ccbu\supporttools*.

This section contains the following topics:

Command-Line Mode vs Interactive Mode

When run from a command line, Web Tools can be run in either command-line mode or interactive mode:

- In command-line mode, you enter the command invoking the utility, along with specific arguments, on a single line. After the command executes the utility automatically exits.

  Example: `c:\cisco\ccbu\supporttools> interrogate /system logger_a / query`

- In interactive mode, you enter the command invoking the utility on a separate command line. After that, you can enter as many successive commands as desired. The utility does not terminate until you explicitly quit.

  `c:\cisco\ccbu\supporttools> interrogate`

  `> system logger_a`

  `> query`

  `> quit`

Note: The trace and Log utilities are only available in batch mode; they cannot be used in command-line or interactive mode.

Selecting a System to Use

When run from a command line, unless otherwise specified, Web Tools assume that the local machine is both:

A) The application server (the machine from which the utility should be run), and

B) The target system (the machine to be queried by the utility).

For example, to run the System Interrogate utility on the local machine, and to target its query at that same machine, enter:

`>interrogate /query`

Selecting a Different Application Server

If desired, you can specify a different machine (other than the local one) from which to run a utility. For example, to run the System Interrogate utility from a machine named logger_a, enter:

`>interrogate logger_a`

```
>query
```

Selecting a Different Target System

If desired, you can use the /system option to specify a different machine as the target system of a command. The /system option can only be used when the application server is a Support Tools Server; You cannot target a remote system when using a node as your application server.

For example, to target a System Interrogate query at a machine named logger_b, enter:

```
>interrogate
```

```
>system logger_b
```

```
>query
```

Note: This command is not available for the Log Group and Log Collection utilities. In those utilities, the target system specification is built into the log group(s) being used in the request.

Viewing a list of targetable systems

Once connected to an application server, you can use the systemlist (or syslist) command to view a list of all systems that can be selected for targeting. Use the /check option with systemlist to verify connection status to available systems.

For example, entering systemlist /check returns output such as:

```
Hostname: IP Address: System Type: Connection:
```

```
10.86.128.84 10.86.128.84 ICM c
```

Note: The systemlist /check option uses the character **c** for valid and **x** for invalid.

Saving, Viewing, and Retrieving Files

Most Web Tools allow you to save, view, and download files from the Support Tools Repository. Each Support Tools node has its own local Repository. When using Web utilities from a command line on a node, the Repository in use is the Repository on that node (or whatever machine has been specified as the application server).

Getting Help for Command Line Tools

Use the **cmdhelp** or **chelp** command to view a complete list of options for any tool.

To view usage for a specific command, enter: **<command_name> /?**.

Embedded Spaces

In command-line arguments, remember to place paths, file names, etc. that contain embedded spaces in quotes. Failure to do this will prevent a command from executing correctly.

Example: `> view "my file.txt"`

How to Use the Services Utility from a Command Line

While primarily designed for use from the Support Tools Dashboard, the Services utility can also be run from a command line any node, as desired.

Use the Services utility to:

- View information on all services installed on a system

- Stop or start services on a system

- Save a list of services to a file

To Access the Services Utility from a Command Line

To run the Services utility in interactive mode from a command line:

Step 1 From a command prompt on a Support Tools node, navigate to `<support_tools_root>`.

Step 2 Enter `servicecontrol`. Optionally in the same line, to specify a different machine to serve as the application server, enter its DNS or IP address. If none is specified, the local machine serves as the application server. Press `<Enter>`.

Note: To view a list of systems defined in the current system's system list, use the `systemlist` command. To view connection status for systems in the list, use the `systemlist /check` command.

Step 3 Enter commands as described in the Command Line Options section below.

Note: For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see Using Cisco Common Tools from a Command Line (page 125).

Using the Services Utility from a Command Line

When using the Services utility from a command line, note that:

- Unlike in Dashboard use, you can stop services whose Type is Critical (service type is defined in the user-modifiable **processinfo.xml** file.)\

- Prior to stopping a service, you should be aware of the significance of stopping it, including any dependant services that may be affected.

- The Services utility will not allow you to stop services with peer or child dependencies while those dependencies are running. If you attempt to stop such a service, the utility returns a message stating that dependent services are running.

Table 5: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility. **Note:** Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	`>cmdhelp`
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> / <options>`
system	Specifies the target system the utility should run against. If not specified, the utility is run against the local system.	`> /system <host_name> / <options>`
localhost	Sets the network address of name of the target node to the local host. **Note:** By default, unless a different system is specified (using the system command) the local host is assumed to be the target system.	`>localhost`

list	Displays information on all services on the target system.
	
	For each service, this command displays:
	
	- Service Name: The service's name.
	
	- PID: The service's process ID.
	
	- Type: Critical, Known, or Unknown, as defined in the target system's processinfo.xml file.
	
	- Start (if the process is stopped) or Stop (if the process if started.
		`>list`
		
		OR
		
		`>list <localfile_path\filename>`

How to Use the Services Utility from a Command Line

Command:	Description:	Example:
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.	
start	Starts a stopped service on the target system.	`>start <pid> <service_name>` **Note:** Enter "0" for the PID when starting a service.
stop	Stops a started service on the target system.	`>stop <pid> <service_name>`

save	Saves the latest list command results to a services file in the application server's Repository.
	
	Saved output is stored as XML-formatted text.
	
	If no file name is specified, output is saved to a file named: ServicesList <host_name> <timestamp>.xml.
	
	Optionally, you can include an argument that specifies a file name.
		`>save`
		
		OR
		
		`>save <filename>`

files	Displays the list of services files in the application server's Repository.	`>files`

view	Displays the contents of a services file from the Repository on the application server.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>view <filename>`
		
		OR
		
		`>view <filename> <localfile_path\filename>`

remove, rm	Deletes a specified services file from the Repository on the application server.	`>remove <filename>`
rename, ren	Renames a services file in the Repository on the application server.	`>rename <filename> <new_filename>`
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	Executes command without displaying output. **Note:** Available in command-line mode only.	`><command> /silent`
quit, q	Ends the program.	`>quit`

Viewing and Stopping a Service - Examples

The following table shows an example of viewing and stopping a service, with a description of each entry.

Command Option:	Description:
>servicecontrol	Invokes the Services utility.
>list	Returns a list of all services installed on the target system, along with their current status.
>stop 01464 "snmp service"	Stops the specified service. **Note:** Due to an embedded space, the service name was placed in quotes The process ID example "01464" may be different each time a process is run.

How to Use the Processes Utility from a Command Line

While primarily designed for use from the Support Tools Dashboard, the Processes utility can also be run from a command line any node, as desired.

Use the Processes utility to:

- View all processes running on a system

- Terminate processes on a system

- Save a list of processes to a file

To Run the Processes Utility from a Command Line

To run the Processes utility in interactive mode from a command line:

Step 1 From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2 Enter **processcontrol**.

To view a list of systems defined in the current system's system list, use the systemlist command. To view connection status for systems in the list, use the systemlist **/check** command.

Step 3 Enter commands as described in the Command Line Options section below.

> **Note:** For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see Using Cisco Common Tools from a Command Line (page 125).

Using the Processes Utility from a Command Line

When using the Processes utility from a command line, note that unlike in Dashboard use, you can stop processes whose Type is Critical (service type is defined in the user-modifiable **processinfo.xml** file.)

Table 6: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility. **Note:** Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	`>cmdhelp`
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> /` `<options>`
system	Specifies the target system the utility should run against. If not specified, the utility is run against the local system.	`> /system <host_name> /` `<options>`
localhost	Sets the network address of name of the target node to the local host. **Note:** By default, unless a different system is specified (using the system command) the local host is assumed to be the target system.	`>localhost`

list	Displays information on all processes on the target system.
	
	For each proccess, this command displays:
	
	• proccess Name: The process's name.
	
	• PID: The process's process ID.
	
	• Type: Critical, Known, or Unknown, as defined in the target system's processinfo.xml file.
	
	• Start (if the process is stopped) or Stop (if the process if started.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>list`
		
		OR
		
		`>list`
		`<localfile_path\filename>`

Command:	Description:	Example:
kill	Terminates a started process on the target system.	`>stop <pid> <process_name>`

save	Saves the latest list command results to a processes file in the application server's Repository.
	
	Saved output is stored as XML-formatted text.
	
	If no file name is specified, output is saved to a file named: Processes list <host_name> <timestamp>.xml.
	
	Optionally, you can include an argument that specifies a file name.
		`>save`
		
		OR
		
		`>save <filename>`

files	Displays the list of precesses files in the application server's Repository.	`>files`

view	Displays the contents of a precesses file from the Repository on the application server.	`>view <filename>`
		
		OR
		
		`>view <filename> <localfile_path\filename>`

remove, rm	Deletes a specified precesses file from the Repository on the application server.	`>remove <filename>`
rename, ren	Renames a precesses file in the Repository on the application server.	`>rename <filename> <new_filename>`
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	Executes command without displaying output. **Note:** Available in command-line mode only.	`><command> /silent`
quit, q	Ends the program.	`>quit`

Viewing and Killing a Service - Examples

The following table shows an example of viewing and killing a process, with a description of each entry.

Command Option:	Description:
`>processcontrol`	Invokes the Processes utility.

Command Option:	Description:
`>list`	Returns a list of all precesses installed on the target system, along with their current status.
`>stop 01464 "snmp service"`	Stops the specified service. **Note:** Due to an embedded space, the service name was placed in quotes The process ID example "01464" may be different each time a process is run.

How to Use the System Interrogate Utility from a Command Line

While primarily designed for use from the Support Tools Dashboard, the System Interrogate utility can also be run from a command line any node, as desired.

Use the System Interrogate utility to:

- View detailed information about a system's OS, hardware, ICM, and third-party products.

- Save current system information to a file

To Run the System Interrogate Utility from a Command Line

To run the System Interrogate utility in interactive mode from a command line:

Step 1 From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2 Enter `interrogate`.

To view a list of systems defined in the current system's system list, use the systemlist command. To view connection status for systems in the list, use the systemlist `/check` command.

Step 3 Enter commands as described in the Command Line Options section below.

Note: For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see .

Using the System Interrogate Utility from a Command Line

Table 7: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility.	`>cmdhelp`

Command:	Description:	Example:
	Note: Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> /` `<options>`
system	Specifies the target system the utility should run against. If not specified, the utility is run against the local system.	`> /system <host_name> /` `<options>`
localhost	Sets the network address of name of the target node to the local host. **Note:** By default, unless a different system is specified (using the system command) the local host is assumed to be the target system.	`>localhost`

query, qry	Displays detailed information about the target system.
	
	For a detailed listing of displayed information, see How to Use the System Interrogate Screen.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>query`
		
		OR
		
		`>qry`

save	Saves the latest query command results to a file in the application server's Repository.
	
	Saved output is stored as XML-formatted text.
	
	If no file name is specified, output is saved to a file named: SysQuery <host_name> <timestamp>.xml.
	
	Optionally, you can include an argument that specifies a file name.
		`>save`
		
		OR
		
		`>save <filename>`

files	Displays the list of System Interrogate files in the target system's Repository.	`>files`

view	Displays the contents of a System Interrogate file from the Repository on the application server.	`>view <filename>`
		
		OR
		
		`>view <filename>` `<localfile_path\filename>`

Command:	Description:	Example:

download, dl	Downloads a local copy of a System Interrogate file from the application server's Repository.
	
	Optionally, you can include a /text argument to convert the file from XML-formatted text to plain text.
		`>download`
		`<repository_filename>`
		`<local_filename> /text`
		
		OR
		
		`>download`
		`<repository_filename>`
		`<localfile_path\filename>`
		`/text`

remove, rm	Deletes a specified System Interrogate file from the Repository on the application server.	`>remove <filename>`
rename, ren	Renames a System Interrogate file in the Repository on the application server.	`>rename <filename>` `<new_filename>`
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	Directs command input to another input file. **Note:** Available in command-line mode only.	`><command> /silent`
quit, q	Ends the program.	`>quit`

Viewing System Information - Examples

The following table shows an example of querying system information, with a description of each entry.

Command Option:	Description:
`>interrogate`	Invokes the System Interrogate utility.
`>query`	Queries the target system. Returns detailed on that system.

How to Use the Registry Utility from a Command Line

While primarily designed for use from the Support Tools Dashboard, the Registry utility can also be run from a command line any node, as desired.

Use the Registry utility to:

- View the ICM Windows registry settings for the current system

- Save registry settings to a file

To Run the Registry Utility from a Command Line

To run the Registry utility in interactive mode from a command line:

Step 1 From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2 Enter **registry**.

To view a list of systems defined in the current system's system list, use the systemlist command. To view connection status for systems in the list, use the systemlist **/check** command.

Step 3 Enter commands as described in the Command Line Options section below.

Note: For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see Using Cisco Common Tools from a Command Line (page 125).

Using the Registry Utility from a Command Line

Table 8: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility. **Note:** Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	`>cmdhelp`
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> / <options>`
system	Specifies the target system the utility should run against. If not specified, the utility is run against the local system.	`> /system <host_name> / <options>`
localhost	Sets the network address of name of the target node to the local host. **Note:** By default, unless a different system is specified (using the system command) the local host is assumed to be the target system.	`>localhost`

How to Use the Registry Utility from a Command Line

Command:	Description:	Example:

list	Displays the ICM Windows Registry setting for the target system.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>list`
		
		OR
		
		`>list`
		`<localfile_path\filename>`

instance	Used in conjunction with the list command, specifies the customer instance whose registry values will be returned. If not specified, the List command automatically returns registry values for the first customer instance it finds on the target system.	`>/list /instance` `<instance_name>`

save	Saves the latest list command results to a registry file in the application server's Repository.
	
	Saved output is stored as XML-formatted text.
	
	If no file name is specified, output is saved to a file named: Registry <host_name> <timestamp>.xml.
	
	Optionally, you can include an argument that specifies a file name.
		`>save`
		
		OR
		
		`>save <filename>`

files	Displays the list of registry files in the application server's Repository.	`>files`

view	Displays the contents of a registry file from the Repository on the application server.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>view <filename>`
		
		OR
		
		`>view <filename>`
		`<localfile_path\filename>`

remove, rm	Deletes a specified registry file from the Repository on the application server.	`>remove <filename>`
rename, ren	Renames a registry file in the Repository on the application server.	`>rename <filename>` `<new_filename>`
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	Directs command input to another input file. **Note:** Available in command-line mode only.	`><command> /silent`

Command:	Description:	Example:
quit, q	Ends the program.	`>quit`

Viewing Registry Information - Examples

The following table shows an example of querying registry information, with a description of each entry.

Command Option:	Description:
`>registry`	Invokes the Registry utility.
`>list /instance customer_1`	Queries the local system and returns the registry information for a customer instance named customer_1. If a specific instance in not specified, the List command automatically returns registry values for the first customer instance it finds on the target system.
`>save`	Optionally, saves the data returned to a registry file in the application server's Repository. If no file name is specified, output is saved to a file named: Registry <host_name> <timestamp>.xml. Optionally, you can include an argument that specifies a file name.

How to Use the Compare Registries Utility from a Command Line

While primarily designed for use from the Support Tools Dashboard, the Compare Registries utility can also be run from a command line any node, as desired.

Use the Compare Registries utility to:

- Compare the ICM Windows registry settings between:

  – The current system and another system

  – The current system and a registry file stored in the Support Tools repository

  – Two registry files in the repository

- Copy registry values from one system to another, or from a file to the current system

  Save a comparison to a file in the Repository

To Run the Compare Registries Utility from a Command Line

To run the Compare Registries utility in interactive mode from a command line:

Step 1   From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2   Enter `regcompare`.

To view a list of systems defined in the current system's system list, use the systemlist command. To view connection status for systems in the list, use the systemlist `/check` command.

Step 3   Enter commands as described in the Command Line Options section below.

Note: For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see Using Cisco Common Tools from a Command Line (page 125).

Using the Compare Registries Utility from a Command Line

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility. **Note:** Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	`>cmdhelp`
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> /` `<options>`
system	Specifies the target system the utility should run against. If not specified, the utility is run against the local system.	`> /system <host_name> /` `<options>`
localhost	Sets the network address of name of the target node to the local host. **Note:** By default, unless a different system is specified (using the system command) the local host is assumed to be the target system.	`>localhost`

Command:	Description:	Example:

compare, comp
 	
./systems
 	
./files
 	
./system2file
	Compares the contents of two registries and displays the result.
	
	You can compare:
	
	• The current system to a different system
	
	• Two registry files in the Repository
	
	• The current system to a registry file in the Repository
	
	• Any of the above, but only view the differences between the two commands.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
	
	When viewing results:
	
	• Values whose data are identical in both systems are prefaced by Common Value =
	
	• Values whose data are unique to the current system are prefaced by SRC =
	
	• Values whose data are unique to the current system are prefaced by SRC =
		`>compare /systems <2nd system>`
		
		OR
		
		`>compare /file <reg_file_1> <reg_file_2>`
		
		OR
		
		`>compare /system2file <reg_file>`
		
		To see only differences between the two registries, use `/diffonly` at the end of the command.

instance	Used in conjunction with the compare command, specifies the customer instance whose registry values will be compared. If not specified, the List command automatically returns registry values for the first customer instance it finds on each compared system.	`>compare /systems <2nd system> /instance <instance_name>`

apply
 	
/src2diff
 	
/diff2src
	Copies a registry value from one registry to another, or from a file to a registry, using values from the last compare command result.
	
	Use the /src2diff and /diff2src arguments to specify which direction the value should be copied.
	
	Note that you can only copy values to a registry; you cannot copy a value to a file.
		`>apply <keyname> <value> /src2diff`
		
		OR
		
		`>apply <keyname> <value> /diff2src`

save	Saves the latest compare command results to a registry file in the application server's Repository.
	
	Saved output is stored as XML-formatted text.
		`>save`
		
		OR
		
		`>save <filename>`

Command:	Description:	Example:
	If no file name is specified, output is saved to a file named: RegCompare <host_name> <timestamp>.xml. Optionally, you can include an argument that specifies a file name.	
files	Displays the list of RegCompare files in the application server's Repository.	`>files`

view	Displays the contents of a RegCompare file from the Repository on the application server.
	
	Optionally, you can include an argument to dump this output to a local file. Output is stored as XML-formatted text.
		`>view <filename>`
		
		OR
		
		`>view <filename>`
		`<localfile_path\filename>`

remove, rm	Deletes a specified RegCompare file from the Repository on the application server.	`>remove <filename>`
rename, ren	Renames a RegCompare file in the Repository on the application server.	`>rename <filename>` `<new_filename>`
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	Executes command without displaying output. **Note:** Available in command-line mode only.	`><command> /silent`
quit, q	Ends the program.	`>quit`

Compare Registries - Examples

The following table shows a sample registry comparison request, with a description of each entry.

Table 9: Example - Performing a Registry Comparison

Command Option:	Description:
>registry	Invokes the Registry Comparison utility.
>compare /systems logger_b /instance customer_1	Specifies that the local system's registry settings for customer instance_1 be compared to logger_b's settings for that instance.

Command Option:	Description:
	If a specific instance in not specified, the compare command automatically returns registry values for the first customer instance it finds on each system. Note that in some cases these may not be identical instances.
>save	Optionally, saves the data returned to a regcompare file in the application server's Repository. If no file name is specified, output is saved to a file named: Registry <host_name> <timestamp>.xml. Optionally, you can include an argument that specifies a file name.

The following table shows a sample of copying a registry key value from on system to another. Prior to running this command, you must first perform a registry comparison, as shown in the previous example.

Table 10: Example - Copying Key Values from one Registry to Another

Command Option:	Description:
>apply "HKEY_LOCAL_MACHINE\\SOFTWARE\\Cisco Systems, Inc.\\CCBU\\Support Tools\\Tools\\SysQuery" ProgID /src2diff	Specifies that the value ProgID for key HKEY_LOCAL_MACHINE\\SOFTWARE\\Cisco Systems, Inc.\\CCBU\\Support Tools\\Tools\\SysQuery should be copied from the target system to the system specified in the Compare command (in the previous example). **Note:** The key name has been placed in quotes because it included embedded spaces.

How to Use the Log Groups Utility from a Command Line

Use the Create Log Group Screen to:

- Create log groups

- View details of log groups

- Edit log group definitions

- Rename log groups

- Delete log groups

To Run the Log Groups Utility from a Command Line

To run the Log Groups utility in interactive mode from a command line:

Step 1   From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2   Enter `lgtool`.

Step 3   Enter commands as described in the Command Line Options section below.

Note: For additional information on basic Web Tools command line use, including system selection options and command-line mode vs interactive mode see Using Cisco Common Tools from a Command Line (page 125).

Using the Log Groups Utility from a Command Line

Table 11: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility. **Note:** Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	`>cmdhelp`
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`><app_servername> /` `<commands>`
system	**Note:** This command is not used with the Log Groups utility.	
localhost	**Note:** This command is not used with the Log Groups utility.	
create_log_group, clg	Opens a session for creating a log group and specifies the new group's name.	`>clg <new_group_name>` **Note:** Maximum length for name is 32 characters.
list_products, lpd	Displays products that can be selected for log collection.	`>lpd`

Command:	Description:	Example:
list_systems, lsys	Displays systems that can be selected for log collection. For each system for which the information is available, it displays: • product • system name • customer name • icm or ccm node name • process name	`>lsys`

add_log, al
 	
/product
 	
/system
 	
/icm_customer
 	
/icm_node
 	
/icm_process
 	
/ccm_node
	Adds one log in the current log group.
	
	• For ICM logs you must specify: /product, /system, /icm_customer, /icm_node, and /icm_process.
	
	• For CCM logs you must specify: /product, /system, and /ccm_node.
	
	• For CEM, CCM, and CCS logs, you must specify: /product and /system.
		`>al /product ICM /system`
		`<system_name> /`
		`icm_customer`
		`<customer_name> /`
		`icm_node <node_name> /`
		`icm_process`
		`<process_name>`
		
		`>al /product CCM /system`
		`<system_name> /ccm_node`
		`<node_name>`
		
		`>al /product CCS /system`
		`<system_name>`

remove_log, rl	Removes a log from current log group.	`rl <log_name>`
list_selected_log, lsl	Displays logs included in the current log group.	`>lsl`
log_group_description, lgdesc	Optionally, sets a description for the current log collection.	`>lgdesc <description>`
close_log_group, closelg /save	Closes and saves the current log group to the application server's Repository. When closing a new group, closelg automatically saves the group. When closing an existing group that was opened for editing, you must explicitly choose save by entering: closelg /save YES. To close without saving, enter: closelg /save NO.	`>closelg`
list_log_groups, lslg	List all log groups in the application server's Repository.	`>lslg`

Command:	Description:	Example:
display_log_group, dlg	Displays details of a log group from the application server's Repository.	`>dlg <log_group_name>`
open_log_group, openlg	Opens a log group for editing from the application server's Repository.	`>openlg <log_group_name>`
remove_log_group, rmlg	Deletes a log group from the application server's Repository.	`>rmlg <log_group_name>`
rename_log_group, renlg	Renames a log group in the application server's Repository.	`>renlg <old_group_name> <new_group_name>` **Note:** Maximum length for name is 32 characters.
xml	**Note:** This command is not used with the Log Groups utility.	
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility.	`>read <filename>`
silent	**Note:** This command is not used with the Log Groups utility.	
quit, q	Ends the program.	`>quit`

Creating a Log Group - Examples

The following table shows a sample log group creation, with a description of each entry.

Command Option:	Description:
>lgtool	Invokes the Log Group utility.
>clg my_log_group	Initiates a request for a new group and specifies the group name.
>lsys	Displays a list of systems, instances, nodes, and processes whose logs can be added to the group.
>al /product ICM /system 192.168.2.199 /icm_customer customer_1 /icm_node LoggerA /icm_process csfs	Adds an ICM log to the group request.

Command Option:	Description:
>al /product CCS /system CollServer001	Adds a second (CCS) log to the group. Each log must be added on a separate line.
>lgdesc my_group_description	Optionally, creates a description of the group.
>closelg	Closes the log group and saves it to the application server's Repository.

How to Use the Log Collection Utility from a Command Line

Use the Log Collection utility to:

- Create a log collection

- Download collected logs

- View details of log collections

- Delete log collections

Note: The Log Collection utility can be run in interactive mode only; command-line mode is not available for this tool. For additional information on basic Web Tools command line use, including the distinction between command-line mode and interactive mode, see Using Cisco Common Tools from a Command Line (page 125).

To Run the Log Collection Utility from a Command Line

To run the Log Collection utility from a command line:

Step 1   From a command prompt on a Support Tools node, navigate to <support_tools_root>.

Step 2   Enter `lctool`.

Step 3   Enter commands as described in the Command Line Options section below.

Using the Log Collection Utility from a Command Line

Table 12: Command Line Options

Command:	Description:	Example:
cmdhelp, chelp	Displays a list of commands specific to this utility.	`>cmdhelp`

How to Use the Log Collection Utility from a Command Line

Command:	Description:	Example:
	Note: Using Help or ? also displays this list, but includes several additional ICM commands (e.g., echo, error_stop) not used by this utility.	
/?	Displays syntax for a specified command.	`><command> /?`
appserver	Optionally Specifies the system on which the utility should run. If not specified, the utility is run on the local system.	`>lctool <app_servername>`
system	**Note:** This command is not used with the Log Collection utility.	
localhost	**Note:** This command is not used with the Log Collection utility.	
create_collection_request, ccolreq	Opens a session for creating a log collection request and specifies the new collection's name.	`>ccolreq <new_collection_name>` **Note:** Maximum length for name is 32 characters
add_log_group, alg	Adds one log group from the application server's Repository into current log collection. Each log group must be added on a separate line.	`>alg <log_group_name>`
remove_log_group, rmlg	Removes 1 log group from current log collection.	`>rmlg <log_group_name>`
list_log_groups, lslg	Lists the log groups in the current collection request.	`>lslg`
add_request_description, lcdesc	Optionally, sets a description for current log collection.	`>lcdesc <description>`
set_icm_binary, bin /on /off	Optionally, sets the icmBinary flag ON or OFF. ON causes ICM logs to include binary data. If not specified, defaults to off.	`>bin /on`

set_log_range, range
 	
/start_date
 	
/start_time
 	
/end_date
 	
/end_time
	Specifies the date/time range for logs to collect. /start_date, /start_time, /end_date and /end_time are all required.
	
	Date format is mm/dd/yyyy. Time format is hh:mm.
	
	Optionally, you can specify /all in place of specific dates/times.
		`>range /start_date mm/ dd/yyyy`
		
		`/start_timehh:mm / end_date mm/dd/yyyy`
		
		`/end_time hh:mm`

Command:	Description:	Example:
/all		
set_merge_logs, merge /off /on	Optionally, set merge flag ON or OFF. On causes logs to be merged. If not specified, defaults to off.	`>merge /on`
submit_collection_request, submit	Submits the current collection request to application server to start the log collection.	`>submit`
discard_collection_request, discard	Discards and closes the current collection request without exiting the Log Collection utility.	`>discard`
list_logs, lslc	List information, including status, of all log collections in the application server's Repository.	`>lslc`
view_collection, view	Displays detailed information of a specified log collection.	`>view <collection_name>`
remove_log, rmlc	Deletes log collection from the application server's Repository.	`>rem <collection_name>`

rename_log, ren	Renames a log collection in the application server's Repository.	`>ren <old_collection_name>`
		
		`<new_collection_name>`
		
		Note: Maximum length for name is 32 characters

download_log, download /filename /index	Downloads a specified log file from the application server's Repository to a local drive.	`download`
xml	**Note:** This command is not used with the Log Collection utility.	
read_file, read	Directs command input to another input file. For example, you can direct input to run a batch file that contains a series of commands executable by this utility	`>read <filename>`
silent	**Note:** This command is not used with the Log Collection utility.	

Command:	Description:	Example:
quit, q	Ends the program.	`>quit`

Log Collection - Examples

The following table shows a sample log collection request, with a description of each entry.

Table 13: Creating a Log Collection Request

Command Option:	Description:
>lctool	Invokes the Log Collection utility.
>ccolreq my_collection_name	Initiates a request for a new collection and specifies the collection name.
>alg log_group_1	Adds a log group from the application server's Repository to the request.
>alg log_group_2	Adds a second log group to the request. Each group must be added on a separate line.
>lcdesc my_collection_description	Optionally, creates a description of the request.
>range /start_date 09/01/2006 /start_time 00:00 /end_date 09/01/2006 /end_time 00:00	Specifies the date/time range for logs to collect. /start_date, /start_time, /end_date and /end_time are all required. Date format is mm/dd/yyyy. Time format is hh:mm. Optionally, you can specify /all in place of specific dates/times.
>bin on	Optionally, specifies that binary data should be included in the logs. If not specified, defaults to Off. **Note:** Applies to ICM products only. CCM, CMB, CEM, and CCS are not affected by this option.
>merge on	Optionally, specifies that logs should be merged. If not specified, defaults to Off.
>submit	Submits the request.

The following table shows a sample log download request, with a description of each entry.

Note that you must download a log in order to view it. You cannot view collected logs directly from the Repository.

Logs download to the local machine, regardless of whether this is the machine currently serving as your application server.

Table 14: Downloading Collected Logs

Command Option:	Description:
>lctool	Invokes the Log Collection utility.
>ccolreq my_collection_name	Initiates a request for a new collection and specifies the collection name.
>view my_collection	Displays all of the logs collected by a particular collection. You must use the view command prior to downloading a file. Returns output such as shown below. Note the unique index number (0, 1,2) prefacing each log in the collection: Name: "my_collection" Creation time: Thu Sep 2 11:28:17 2006 Description: Merge: false Binary for ICM Log: false Selection type: all Including Log Group: [my_group] Collected item: 0) ICM : 10.86.128.84 nam50, RouterA, dba 1) ICM : 10.86.128.84 nam50, RouterA, et 2) ICM : 10.86.128.84 nam50, RouterA, mds
>download /index 0 /filename c:\my_collection.zip	Specifies that the log whose index value is 0 should be downloaded from the Repository and saved to the local C drive in a file named my_collection.zip. **Note:** • To download all logs in the collection, omit the/index option. • You can name the downloaded file anything you like. Its file type, regardless of the extension specified, is always Zip.

How to Use the Log Collection Utility from a Command Line

Part 6: Using Cisco Common Tools

Cisco Common Tools are a set of Cisco-authored utilities designed for use with the Cisco components supported by Support Tools.

Most Cisco Common Tools are command-line based, and can be run from either the Support Tools Dashboard or from an individual node. Command-line access to individual nodes can be local or remote (via methods like TelNet, pcAnywhere, etc.).

Several Cisco Common Tools are GUI-based. While menu commands for these utilities appear in the Support Tools Dashboard, they cannot in fact be launched from there. Access to these tools is limited to the individual node (either locally or via remote GUI such as pcAnywhere). These GUI-based Cisco tools include:

- icmdba

- rtrtrace

- ss7nictrace

For the most part, Cisco Common Tools are installed on core ICM components only: AWs, PGs, Call Routes, and Loggers. Not every utility is installed on every node. For example, CICMan is only present on NAM Call Routers. See the table in the next section for more information.

If you attempt to launch a utility that is not present on the current system, the Support Tools Dashboard returns a response identical to the response you would get if you tried to spawn a non-present utility from a command prompt.

Table 15: Cisco Common Tools at a Glance

Utility Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
cicman	Use on a NAM CallRouter to view and set NAM to CICM session information.	NAM Call Routers		
ctitest	Use for debugging or demonstration in a Cisco ICM CTI environment. Can be used in place of an Interactive CTI client application.	CTIOS PGs	X	
dbdiff	Third-party (Microsoft) tool to compare database tables. Invoked with the diffconfig.bat tool.	Nodes on which SQL Server is installed		

Utility Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
dumpcfg	Dump Config ICM audit utility. Use to analyze the ICM Config_Message_Log table. Allows you to determine WHO did WHAT, WHEN, from WHERE, using WHICH program.	Loggers (but can be run from any ICM component)		
icmdba	ICM Database Administration tool. Use to create, monitor, and edit ICM databases, including Logger, HDS, and AWDB databases. ICMDBA is also used to manage various SQL Server operating parameters.	AWs, Loggers (ICM components with DBs)		X
mptrace	Use to provide a playback from the Nortel Meridian Automatic Call Distributor (ACD) to troubleshoot potential issues.	MerPim PGs		
nicroi	NIC Remote Operator Interface. Use to configure and debug the (old-style DOS-based) AT&T NIC. Often invoked with the NIC.BAT batch program.	Routers for customers running an AT&T NIC	X	
nmstart	Node Manager Start. Use to start an ICM service on a CallRouter, Logger, AW, or PG.	AWs, PGs, Call Routers, Loggers	X	
nmstop	Node Manager Stop. Use to stop an ICM Service on a CallRouter, Logger, AW, or PG.	AWs, PGs, Call Routers, Loggers	X	
opctest	Use to interpret a Peripheral Gateways (PG) status, statistics, etc. It is also possible to enable specific debug tracing in the OPC process.	PGs	X	
procmon	General-purpose debugging tool. Can be used in conjunction with various Network Interface Controller (NIC) and Peripheral Interface Manager (PIM) processes. Use to verify status, set debug trace bits, etc.	PGs, Call Routers	X	
rtrtrace	Use to set various debug tracing on a CallRouter. The additional tracing is output to the .EMS log files, and viewed with the Trace and Log tools..	Call Routers		X
rttest	Use to interpret a Call Router's events and states live without interruption to the running router processes. Rttest has several subroutines that allow viewing status, statistics, etc. It is also possible to enable specific debug tracing in the call router.	Call Routers (but can be run from any ICM component)	X	

Utility Name:	Description:	Installed On:	Dashboard Privileged Users Only:	External GUI--No Dashboard or Command-Line Access:
ss7nictrace	Use to view and set various debug trace bits on a new style NT SS7 NIC PG.	PGs		X
vrutrace	Use to output tracing information from a Voice Response Unit (VRU) device and to and from its PIM process. VRUTrace allows capture and playback of session data.	VRU PGs		

Chapter 13

Using Cisco Common Tools

How to Use the CICMan Utility

Use the CICMan utility to view and set NAM to CICM session information for a NAM CallRouter. For use with NAM Call Routers only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access CICMan from the Dashboard

To run CICMan from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > CICMan.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the cicman command is already implied. Do not enter it in the Arguments field.

Step 4   If desired, in the Commands field, enter (or paste from a batch file) a group of commands to run in batch mode.

When you do this:

- Separate individual commands by a new line.

- Do not enter input flags.

- Do not enter an input file name in the arguments field.

Step 5   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 6   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 7   Click the Run button.

To Access CICMan from a Command Line on a Node

From a command-line on a NAM Call Router, you can run CICMan from the ICM root directory. For example:

```
c:\><icm_root>\cicman
```

Using CICMan - Command line Options

Syntax: `cicman [/f InputFile] [/system SystemName] [/cust Customer] [/node ICMNode] [/pipe OutputPipe] [/debug] [/stop] [/help] [/?]`

Parameter Descriptions

- cicr_meters, cmeters: Displays the CICR meters for both CIC sides.

- echo: Controls echoing of command lines

- error_stop: Controls setting of stop on error flag.

- glbl_meters, gmeters: Displays the global meters for both CIC sides.

- help, ?: Display program description.

- link_ctrl, lctrl: Used in upgrade to shut down all links 1-on a CIC A/B or 2-to all CICRs side A/B.

- link_stat, lstat: Displays the link status for both CIC sides.

- quit, q: Ends the program.

- read_file, read: Directs command input to another input file

- table_values, tbl_vals: Displays the CIC Table values including timeouts & thresholds.

How to Use the CTITest Utility

Use the CTITest utility to debug in a Cisco ICM CTI environment. CTITest can be used as an interactive CTI client for demonstration or debugging purposes.

It connects to the CTI Server through a socket connection, and displays either all of the events that are occurring on the switch (a CTI bridge client application), or only the events which pertain to a single agent. If a CTITest has the same configuration that your application does, the expected events and switch behavior is seen in the CTITest program.

For use with CTIOS PGs only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access CTITest from the Dashboard

To run CTITest from the Support Tools Dashboard:

Step 1 Use the System Select screen to select the system (namely, PG) you want to work with.

Step 2 From the Dashboard menu, select Cisco Common Tools > CTITest.

Step 3 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the **ctitest** command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access CTITest from a Command Line on a Node

From a command-line on a CTIOS PG, you can access CTITest from any location on the local physical drive. For example:

```
c:\>ctitest
```

```
d:\temp>ctitest
```

Using CTITest - Configuring

Starting CTITest requires:

- The CTI Server (PG) IP address

- The socket number

- The agent ID and login information

Note: In addition to ctitest.exe, trace dll (icrmsgs.dll) is also located in the <icm_root>\bin directory. Because icrmsgs.dll is an active services file, it is recommended that these two files be copied into separate directory.

Step 1   Set up a profile which consists of settings used as input to CTITest. To initiate a new profile, start the CTITest with the following command: **c:\abc\>ctitest /p <profile name>**

Step 2   Configure the CTI Server and socket where the CTITest connects to:

1.   Configuring Side A CTI Server: Run the following command to configure the CTI Server Side A for the CTITest.

     ```
     c:\abc\>ctitest: config /hostA <ctiserver_hostnameA> /portA
     <ctiserver_portA>
     ```

2.   Configuring Side B CTI Server: Run the following command to configure the CTI Server Side B for the CTITest if you have a duplex configuration.

```
c:\abc\>ctitest: config /hostb <ctiserver_hostnameB> /portB
<ctiserver_portB>
```

Note:

- In the above example, <ctiserver_hostnameA> <ctiserver_hostnameB> represents the IP address or host name of the CTI Server or PG side A and B, and <ctiserver_portA> <ctiserver_portB> represents the port number of side A and B.

- If it is a simplex environment, use "" to specify a null value.

Step 3   Configure the CTI protocol version to 6: `c:\abc\>ctitest: config /version 6`

Step 4   Configure the service mask to 7: `c:\abc\>ctitest: config /service 7`

Step 5   It is suggested that you turn off heartbeats while debugging the CTI issues. To configure heartbeat to -1, use the command: `c:\abc\>ctitest: config /hb -1`

Step 6   Configure the agent to determine the desired Client Events for Client Mode. These vary depending on your CTI Server environment: `c:\abc\>ctitest: agent /periph <peripheral_id> /id <agentid> /password <password> /ext <extension> / inst <instrument>`

Note: If there is no agent password required to login, use "" to specify a null value. Run the agent /? command for help.

Using CTITest - Opening a Session

The open command performs a socket connection to the CTI Server, and issues the appropriate commands to the CTI Server to establish message communication. By default, the CTITest repeatedly attempts to open a session until it either opens a session, or the close or quit command is given. It automatically attempts to connect to the other side following a failure of the CTI Server. You can open a session after completing a configuration successfully as described below.

```
c:\abc\>ctitest: open
```

If your CTITest configuration is correct, a message appears similar to the following:

```
session #2 opened after 0 ms CCTime 13:52:32 PGStatus NORMAL Peripheral:
Online
```

If errors are received while opening a session, verify your CTITest configuration as outlined above.

Using CTITest - Logging In

You can login into the Automatic Call Distributor (ACD) that the PG is communicating with, if the session is successfully opened. Below is the syntax for issuing the login command:

Syntax: `CTITest: login /? usage: agent_login ID PASSWORD [/periph N] [/instrument N] [/reason N] [/position N] [/supervisor N] [/auctoIN] [/manualIN] [/skill N[.pri] [/skill N[.pri]] ]`

Based on the type and configuration of the ACD, you need to provide these parameters for a successful login. Once connected, you can change agent states, answer call, transfer call, make call, conference, etc. using CTITest.

Using CTITest - Logging In

Below is list of frequently used commands in CTITest:

Command:	Parameters:
agent_login (login)	`ID PASSWORD [/periph n] [/instrument N] [/reason N] [/position N] [/supervisor N] [/autoIN] [/manualIN] [/skill N[.pri] [/skill N[.pri]] ...]`
agent_logout (logout)	`[/agentID ID] [/password] [/periph n] [/instrument N] [/reason N] [/skill N[.pri] [/skill N[.pri]] ...]`
agent_not_ready (not_ready)	`[/agentID ID] [/periph n] [/instrument N] [/reason N] [/skill N[.pri] [/skill N[.pri]] ...]`
agent_ready (ready)	`[/agentID ID] [/periph n] [/instrument N] [/reason N] [/autoIN] [/manualIN] [/skill N[.pri] [/skill N[.pri]] ...]`
agent_work_not_ready (wrapup)	`[/agentID ID] [/periph N] [/instrument N] [/reason N] [/skill N[.pri] [/skill N[.pri]] ...]`
agent_work_ready (callwork)	`[/agentID ID] [/periph N] [/instrument N] [/reason N] [/skill N[.pri] [/skill N[.pri]] ...]`
answer_call (answer)	`[/periph N] [/callid CALLID.DEVID] [/stack N] [/instrument N]`
autoanswer	`[/on] [/off]`
clear_call (clear)	`[/periph N] [/callid N.devid] [/stack N]`
conference_call (conf)	`[/periph N] [/active CALLID.DEVID] [/held CALLID.DEVID] [/stack ACTIVE HELD] [/blind DN] [/placement TYPE] [/manner TYPE] [/alertRings N] [/callopt TYPE] [/TG N] [/SG N] [/authorize code] [/account code]`
consult_call (cc)	`DN [/periph N] [/instrument N] [/callid N.devid] [/stack N] [/placement TYPE] [/manner TYPE] [/transfer] [/conference]`

Command:	Parameters:
	`[/alertRings N] [/callopt TYPE] [/priority] [/postroute] [/ TG N] [/SG N] [/authorize code] [/account code]`
get_agent_state (state)	`[/periph n] [/instrument N]`
get_agent_stats(stats)	`[/periph N] [/instrument N] [/ext string] [/id string]`
get_skill_stats (sk_stats)	`[/periph N] [/skill N] [/skillID N]`
hold_call (hold)	`[/periph N] [/callid N.devid] [/stack N]`
make_call (mc)	`DN [/periph N] [/instrument N] [/placement TYPE] [/manner TYPE] [/alertRings N] [/callopt TYPE] [/priority] [/ postroute] [/TG N] [/SG N] [/authorize code] [/account code] [keyword=VALUE ...]`
release	`[/periph N] [/callid N.devid] [/stack N]`
retrieve_call (retrieve)	`[/periph N] [/callid N.devid] [/stack N]`
transfer_call (transfer)	`[/periph N] [/active CALLID.DEVID] [/held CALLID.DEVID] [/ stack ACTIVE HELD] [/blind DN][/placementTYPE] [/manner TYPE] [/alertRings N] [/callopt TYPE] [/TG N] [/SG N] [/authorize code] [/account code]`

How to Use the DBDiff Utility

Use the DBDiff utility to perform comparisons of database tables from two different databases. For example, you might want to check that the ICR_Locks table contains the same data on both sides of a Central Controller.

For use with nodes on which SQL Server is installed only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access DBDiff from the Dashboard

To run DBDiff from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system (namely, PG) you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > DBDiff.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the dbdiff command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access DBDiff from a Command Line on a Node

From a command-line on an ICM node on which SQL Server is installed, you can access DBDiff from any location on the drive on which ICM is installed. For example:

`c:\>dbdiff`

`c:\temp>dbdiff`

Using DBDiff

Syntax: `dbdiff <database1.table@host1> <database2.table@host2>`

You can also use the batch script diffconfig.bat to invoke DBDiff for various tables to automatically compare two ICM databases.

Syntax: `diffconfig <database1> <host1> <database2> <host2> <database2.table@host2>`

For example: `diffconfig cust1_sideA geoxyzlgra cust1_sideB geoxyzlgrb`

Command Line Options

Syntax: `DBDiff {database a}.{table a}[@server a] {database b}.{table b}[@server b] [/out:{file}] [/key:{pkey1,pkey2,...}] [/where:"{where clause}"]`

How to Use the DumpCfg Utility

Use the DumpCfg utility to analyze records in the ICM Config_Message_Log table to determine what actions have been performed on an ICM system, when, by whom, and using what applications.

For use with ICM Loggers only, but can be run from any ICM component.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access DumpCfg from the Dashboard

To run DumpCfg from the Support Tools Dashboard:

Step 1 Use the System Select screen to select the system (namely, PG) you want to work with.

Step 2 From the Dashboard menu, select Cisco Common Tools > DumpCfg.

Step 3 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the dumpcfg command is already implied. Do not enter it in the Arguments field.

Step 4 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6 Click the Run button.

To Access DumpCfg from a Command Line on a Node

From a command-line on an ICM Logger, you can access DumpCfg from any location on the local physical drive. For example:

```
c:\>dumpcfg
```

```
c:\>dumpcfg
```

Using DumpCfg

Syntax: `DumpCfg <database>[@server] <low recovery key> [high recovery key]`

How to Use the ICMDBA Utility

Use ICMDBA, the ICM Database Administration tool, to create, monitor, and edit ICM databases, including Logger, HDS, and AWDB databases. You can also use ICMDBA to manage various SQL Server operating parameters.

You can use ICMDBA to:

- Estimate size and bandwidth requirements for databases.

- Create, edit and delete central databases, local databases, and historical database for installed ICM customers.

- Resize database devices.

- Recreate a database.

- Import/export data to/from databases.

- View database properties.

In addition, you can use ICMDBA to start or stop a server, and to do some limited SQL server configuration.

ICMDBA is for use with any ICM component that uses a database (namely, AWs, Loggers).

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Accessing ICMDBA

ICMDBA is an external GUI application present on all ICM nodes as part of that standard ICM installation. It cannot be run from within the Support Tools dashboard.

To access ICMDBA on an ICM component which uses a database (namely, AWs, Loggers), from a command line, enter   `icmdba`.

How to Use the MPTrace Utility

Use the MPTrace utility to get a playback from the Meridian ACD to troubleshoot potential issues. MPTrace provides information on what is configured on the ACD and what needs to be changed. It looks at Controlled Directory Numbers (CDNs) and agent Position IDs/Instrument Identification Numbers (IDNs).

For use with MerPim PGs only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access MPTrace from the Dashboard

To run MPTrace from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > MPTrace.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

        Note: When entering arguments, the mptrace command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access MPTrace from a Command Line on a Node

From a command-line on an ICM MerPim PG, access MPTrace from the merpimcap directory located at: <icm_root>\<customer instance>\<pg#>

For example:

```
c:\icm\my_customer_instance\pg1a\merpincap> mptrace
```

Using MPTrace - Command Line Options

The mptrace command places two text files in the mptrace directory:

- The **pim1_summary** file is a playback of the ACD configuration and includes information on unconfigured Position IDs and CDNs, as well as Meridian Link misconfigurations.

- The **pim1_trace** file is the complete dialog of what the ACD is seeing during this capture.

Note: The pim1_summary and pim1_trace files are overwritten every time MPTrace is used.

When adding new configurations to the ACD, old .cap files from the merpimcap directory should be deleted so that you can see fresh results after new .cap files are written. The .cap files are the raw binary files that are written from the ACD to the merpimcap directory. When an MPTrace is run, these binary .cap files are converted into two text files. If there are old files in the directory, then the playback of the configuration includes old data that may have already been addressed and fixed.

Syntax: **MPTrace [ProcessName(s)] [/if InputFile] [/tf TraceOutputFile] [/sf SummaryOutputFile] [/bd BeginDate(mm/dd/yyyy)] [/bt BeginTime(hh:mm:ss)] [/ed EndDate(mm/dd/yyyy)] [/et EndTime(hh:mm:ss)] [/hr HoursBack] [/all] [/last] [/prev] [/bin] [/ms] [/debug] [/regbase**

```
RegBase] [/icrroot icmRoot] [/pbreal] [/pb_sb PlaybackSecondsToBackup]
[/pb_sync_hh] [/pb_sync_today] [/pb_fsph PlaybackFileStartPositionHint]
[/nobuf] [/notracemlink] [/notracemei] [/tracemlkhex] [/tracemeihex]
[/notracerd] [/notracetp] [/help] [/?]
```

How to Use the NICROI Utility

Use the NICROI (NIC Remote Operator Interface) utility to configure and debug the (old-style DOS-based) AT&T NIC. NICROI allows you to see route request data from the inter-exchange carrier (IXC), and label response information from the Cisco Intelligent Contact Management (ICM) Call Routers.

For use with ICM Loggers for customers running an AT&T NIC only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access NICROI from the Dashboard

To run NICROI from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > NICROI.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the nicroi command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access NICROI from a Command Line on a Node

From a command-line on an ICM Logger for customers running an AT&T NIC, you can access NICROI by entering:

Method 1

```
nic <hostname> 5300 support <customer_instance>xyzzyf
```

For example:

```
c:\>nic my_host_name 5300 support my_customer_instancexyzzy
```

Note: In the example above, support and <customer_instance>xyzzyf represent respectively the out-of-box admin username and password for this utility. Make appropriate substitutions if these values have been modified.

Method 2

```
nic <customer_instance> <nic_extension>
```

For example:

```
c:\>nic my_customer_instance 1a
```

Using Tracing in NICROI

There is only one level of tracing available within NICROI, it allows you to view Route Requests from the carrier. These route requests include the caller's Calling Line ID, any Caller Entered Digits, and the Dialed Digits (same as Dialed Number).

To turn on tracing:

Type nic sfk 4 in the NICROI CONSOLE window. (There is not a prompt in this window, just an empty command line where you may enter commands.) This is the only trace element available within NICROI. You should now be able to click on the activity window behind your NICROI session and see the results of this trace setting scrolling.

To turn off tracing:

In order to turn tracing off, repeat the same entry nic sfk 4.

This added information is then inserted into a log file, either the niclog.xxx or the roilog.txt log file that you open/create. (explained below).

There are two different places that you can capture this data, within the niclog.xxx or within a log file that you must open in order to have data written to it called roilog.txt.

Capturing NICROI Data to niclog.xxx

The niclog.xxx is a file that the NIC writes data to automatically and labels each log file with a date/time stamp, along the same functionality as an EMS log file used for other ICM processes. Use the following steps to view a list of niclog.xxx files:

Step 1   Type **mgmt help** within the NICROI window to see the options available.

Step 2   Type **mgmt file list** to view all the niclog.xxx files available.

Note: The time shown is the time that the log is closed, meaning the time that information stopped being written to that particular log and another log is created. You can see in this list also the size of the file.

Step 3   If you do not see the date and time you are looking for, you can view more log files by typing mgmt file list more until you see the log file that you would like to capture. This log file format is useful if you have several specific time periods that you want to capture.

Capturing NICROI Data to Roilog.txt

The roilog.txt file is a file that is invoked by opening and closing it, this file is NOT automatically generated as the niclog.xxx. This log file is useful if you have one general, extended period of time that you want to capture. Use the following steps to create a roilog.txt file:

To "Open" a roilog.txt file:

From within NICROI issue the log open [<filename>] command. This command causes all status displayed in the NICROI logging window to be stored in a log file on the NICROI host system. The name of the log file can be specified. If omitted, the default name is roilog.txt which is placed in the current directory of the process from which NICROI starts.

Note: If you use this type of log file, you must close the log to stop the writing of information (once you have captured the time frame in question) before you copy the log file out to analyze it.

To "Close" an roilog.txt file:

From within NICROI type the .log command to close the NICROI log file. No further file logging is performed.

Copying NICROI Log Files

You can copy these log files to your local drive. There are basically two ways you can gather this data, based on which file format you choose to use above.

Copying Files Using Roilog.txt

If you have opened and created a log file using the method for roilog.txt, upon closing the log file, you have a copy of the log on your local drive. The file will be located in the directory from which you began your NICROI session. Unless you have specified a download directory using the .xdir c:\<path name> command, then the file is created and written onto your local drive at the location from which you started your NICROI session.

Copying Files Using Niclog.xxx

If you choose to use the niclog.xxx files you need to download or transfer the files to your local drive using the nmg roi transfer command as outlined below. Remember, if you do not specify a transfer directory with the .xdir c:\<path Name> command then the file is transferred to the

directory from which you started your NICROI session. The following two sections are examples of these download commands.

Setting the Download Directory

The .xdir d:\support command allows you to set your download directory so all roilog.txt files created are automatically transferred to that directory as well as any niclog.xxx files downloaded using the nmg roi transfer command (syntax below). If you do not use this command you may still gather these log files. They are then automatically downloaded into the directory from which you started your NICROI session.

Transferring Files

The **nmg roi transfer <file name>** command allows you to transfer niclog.xxx files from NICROI to your local physical drive. Once you execute this command you can see the following lines from within your NICROI session as confirmation that the file transferred correctly.

```
nmg roi transfer <file name>

->BEGIN FILE TRANSFER of <file name>

->TRANSFER: d:\support\<file name> <file size> <date / time / year>

->FILE TRANSFER COMPLETE, seqnum = 3
```

How to Use the NMStart Utility

Use the NMStart (Node Manager Start) utility to start an ICM service on an ICM Call Router, Logger, AW, or PG.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access NMStart from the Dashboard

To run NMStart from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > NMStart.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the nmstart command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access NMStart from a Command Line on a Node

From a command-line on an ICM Call Router, Logger, AW, or PG, you can access NMStart from any location on the local physical drive. For example:

`c:\>nmstart`

`d:\temp>nmstart`

Using NMStart

Syntax: `nmstart <customer_instance> <node>`

For example: `c:\> nmstart cisco pg3a`

How to Use the NMStop Utility

Use the NMStop utility to stop an ICM service on an ICM Call Router, Logger, AW, or PG.

Note:

- This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

- The Support Tools Unknown Process and Services Explorer is an alternate, more robust utility with which to stop ICM services.

To Access NMStop from the Dashboard

To run NMStop from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > NMStop.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the nmstop command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access NMStop from a Command Line on a Node

From a command-line on an ICM Call Router, Logger, AW, or PG, you can access NMStop from any location on the local physical drive. For example:

`c:\>nmstop`

`d:\temp>nmstop`

Using NMStop

Syntax: `nmstop <customer_instance> <node>`

For example: `c:\> nmstop cisco pg3a`

How to Use the OPCTest Utility

Use the OPCTest utility to interpret a Peripheral Gateway's (PG) status, statistics, etc. It is also possible to enable specific debug tracing in the OPC process.

For use with ICM PGs only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access OPCTest from the Dashboard

To run OPCTest from the Support Tools Dashboard: To run OPCTest:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > OPCTest.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the opctest command is already implied. Do not enter it in the Arguments field.

Step 4 If desired, in the Commands field, enter (or paste from a batch file) a group of commands to run in batch mode.

When you do this:

- Separate individual commands by a new line.

- Do not enter input flags.

- Do not enter an input file name in the arguments field.

Step 5 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 6 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 7 Click the Run button.

To Access OPCTest from a Command Line on a Node

From a command-line on an ICM PG, you can access OPCTest from any location on the local physical drive by entering: `opctest /<customer_instance> /<node>`

For example:

`c:\>opctest /my_customer_instance /pg1a`

`d:\temp>opctest /my_customer_instance /pg1a`

Using OPCTest

To list available commands, type help or ? from the OPCTest command prompt.

Some of the OPCTest commands, such as List_Agents and List_Trunk_Group, require one or more additional command line switches. Type command name /? to obtain the proper syntax.

Syntax: `opctest [/f InputFile] [/system SystemName] [/cust Customer] [/ node ICMNode] [/pipe OutputPipe] [/debug] [/stop] [/help] [/?]`

Parameter Descriptions

agent_trace: Controls agent tracing in the router.

call_control, call: Controls various kinds access to OPC calls.

checksum, check: Requests router to do a checksum.

debug_control, debug: Controls various kinds of debugging output from opc.

dump: Requests opc to do a internal state dump to a file.

dump_agent, da: Dump contents of Agent within OPC.

dump_call, dc: Dump OPCs call states.

dump_hash, dh: Display OPCs internal hash statistics.

dump_struct, ds: Requests OPC to dump a structure.

dump_tpservices, dtps: Dump Third Party Service Data object.

echo: Controls echoing of command lines

error_stop: Controls setting of stop on error flag.

exit_opc, exitopc: Sends an message telling the OPC to exit.

expression, expr: Gives the router an expression to evaluate.

help, ?: Displays this help.

list_agents, la: Display OPCs AgentStates for specified Group.

list_calls, lc: Display OPCs call states.

list_routing_client, lrc: Display OPCs Routing Client stats for peripheral.

mem_leaks: Dump memory leakage based on checkpoints from prior calls.

network_trunk_group_trace, ntg_trace: Controls NetworkTrunkGroup tracing in the OPC.

peripheral_trace: Controls Peripheral tracing in the OPC.

quit, q: Ends the program.

read_file, read: Directs command input to another input file

route_call: Sends a route call request to the router.

route_trace: Controls Route tracing in the OPC.

service_trace: Controls Service tracing in the OPC.

skill_group_trace: Controls SkillGroup tracing in the OPC.

status: Sends an message telling OPC to display its status.

stop_log: Requests logmsg to stop logging messages.

trunk_group_trace: Controls TrunkGroup tracing in the OPC.

tuning_param, tune: Controls tuning in the router.

Example

The following example shows detailed output for the **status** command:

Figure 5: OPC Test Example Output

Debug Information

You can enable specific debugging within OPCTest by issuing the debug command. Turning up specific tracing is much more effective than going into the registry, or turning up the EMSTraceMask for the entire OPC process. Enabling debug control turns up tracing on the part of OPC for that you need additional tracing. The tracing result is displayed in the OPC EMS log files. Use the Trace and Log utility to view the output of the EMS logs.

For example:

```
opctest: debug /? Usage: debug_control [/realtime] [/agent] [/halfhour]
[/rcmeter] [/routing] [/skillgroup] [/closedcalls] [/cstaecr] [/cstacer]
[/pimmsg] [/ctimsg] [/rcmsg] [/dmpmsg] [/icmsg] [/opcmsg] [/mdsmsg]
[/pdmsg] [/inrcmsg] [/passthru] [/tpmsg] [/physctrlr] [/periph] [/all]
[/help] [/?]
```

If you need to troubleshoot a translation route problem, try the **debug /routing** command.

Note: The `/noall` switch. Leaving tracing turned up can cause performance problems.

Exiting and Quitting OPCTest

Use the quit command to exit OPCTest.

Warning: Use the `exit_opc` command with caution. This command instructs the OPC process (on both sides of the PG if duplexed) to exit. Node Manager forces the process to restart, which then forces it to reload the configuration for the Call Router. All internal peripheral and agent states are flushed, then OPC and PIM re-learn the PG and its configuration.

How to Use the Procmon Utility

Use the Procmon utility for general-purpose ICM command-line debugging. It can be used in conjunction with various NIC and PIM. processes. Procmon allows you to perform actions like verifying status, setting debug trace bits, and so on.

For use with ICM PGs and Call Routers only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access Procmon from the Dashboard

To run Procmon from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > Procmon.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the opctest command is already implied. Do not enter it in the Arguments field.

Step 4   If desired, in the Commands field, enter (or paste from a batch file) a group of commands to run in batch mode.

When you do this:

- Separate individual commands by a new line.

- Do not enter input flags.

- Do not enter an input file name in the arguments field.

Step 5   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 6   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 7   Click the Run button.

To Access Procmon from a Command Line on a Node

From a command-line on an ICM PG or Call Router, you can access Procmon from any location on the local physical drive. For example:

```
c:\>procmon
```

```
d:\temp>procmon
```

Using Procmon

Procmon supports both local and remote commands. Local commands are defined within Procmon itself, while remote commands are programmed into the monitored process. Below are lists of basic Procmon commands and process-specific commands for use with such processes as PIM, CTISVR and OPC.

Syntax: `PROCMon CustomerName NodeName ProcessName [SystemName] [/f InputFile] [/wait] [/stop] [/help] [/?]`

Procmon Basic Commands

Type help to display the list of basic commands described in the following table.

Command:	Definition:
`echo`	Controls echoing of command lines
`emsmon`	Command to control remote EMS monitor process (start, stop, pause, resume)
`error_stop`	Controls setting of stop on error flag
`help, ?`	Displays this help
`monitor_help, mhelp`	Displays Monitor Server help
`monitor_sleep, msleep`	Sleep for specified seconds or milliseconds

Command:	Definition:
`quit, q`	Ends the program
`read_file, read`	Directs command input to another input file

Procmon Process-Specific and Troubleshooting Commands

Each Peripheral Type contains a different set of commands. For a list of commands associated with each peripheral, use `mhelp`. Each command has its own syntax. to determine the syntax, type the command followed by `/?`.

Command:	Definition:
`pim_list_agents, la`	List agents currently configured by PIM
`pim_list_services, ls`	List Services currently configured by PIM
`pim_list_skill_groups, lsg`	List SkillGroups currently configured by PIM
`acd_debug, debug`	Turn on/off debug trace
`pim_list_trace, ltrace`	List current PIM trace bit settings
`pim_trace, trace`	Set or reset PIM trace bits
`pim_dump_periph, acdperiph`	Dump contents of peripheral object
`Quit`	Ends the Procmon Program

How to Use the RTRTrace Utility

Use RTRTrace to set debug tracing on an ICM CallRouter. The additional tracing is output to the .EMS log files, viewable with the Trace and Log utility.

Router Trace session can be started on either side of a Call Router, and tracing will start logging for both sides when tracing is enabled.

RTRTrace is for use with ICM Call Routers only.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Accessing RTRTrace

RTRTrace is an external GUI application present on all ICM nodes as part of that standard ICM installation. It cannot be run from within the Support Tools dashboard. Online documentation is available from within the RTRTrace GUI.

To access RTRTrace on an ICM Call Router, from a command line, enter `rtrtrace`.

How to Use the RTTest Utility

Use the RTTest utility to interpret a Call Router's events and states without interruption to the running router processes. RTTest has several subroutines that allow you to view status, statistics, and similar information. You can also enable specific debug tracing in the Call Router. By running RTTest, you can quickly get a real time status of the entire ICM system.

For use with ICM Call Routers only, but can be run from any ICM component.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

To Access RTTest from the Dashboard

To run RTTest from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > RTTest.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the `nmstop` command is already implied. Do not enter it in the Arguments field.

Step 4   If desired, in the Commands field, enter (or paste from a batch file) a group of commands to run in batch mode.

When you do this:

- Separate individual commands by a new line.

- Do not enter input flags.

- Do not enter an input file name in the arguments field.

Step 5   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 6   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 7   Click the Run button.

To Access RTTest from a Command Line on a Node

From a command-line on an ICM Call Router, you can access RTTest from any location on the local physical drive. For example:

```
c:\>rttest
```

```
d:\temp>rttest
```

Note: You can access and run RTTest from other ICM components provided that the specified node in the command line argument (see next section) is an ICM Call Router.

Using RTTest

Syntax: `rttest [/f InputFile] [/system SystemName] [/cust Customer] [/node ICRNode] [/pipe OutputPipe] [/debug] [/stop] [/help] [/?]`

The command line options required to invoke RTTest are:

- `cust`: Customer where Customer is a 3, 4, or 5 letter acronym signifying the ICM customer instance.

- `node`: ICM node where ICM node is either routera or routerb, depending on the router RTTest to run.

At the RTTest prompt, type status. It will return the current state of each ICM central site process, ICM Peripheral Gateway server, third-party automatic call distributor (ACD) and Voice Response Unit (VRU) peripheral. For example:

```
c:\> rttest /cust csco /node routera
```

```
rttest:
```

```
rttest: status
```

```
Router Version: Release 2.5 (service pack 2), Build 03134
```

```
Release Date: 12/23/98 13:30:08
```

```
Current Time: 03/17 16:00:42
```

```
Local Time: 03/17 11:00:42 (-5.0 hr)
```

```
Router Up: 02/21 01:01:45 (24.6 day)

Router Sync: 03/11 11:06:20 (6.2 day) (A->B)
```

Status Output: Process

The first section, labeled Process in the first column of the status output, shows the status of each ICM central site process. One ICM central site consists of an ICM call router and an ICM database logger. In most cases there will be two ICM central sites - sideA and sideB for redundancy.

Process:	LastStateChange:	LastHeartBeat:
A agi	- --	
A cic	- --	
A csfs	OK 03/06 11:10:20 (11.2 day)	
A dba	OK MH 03/06 11:10:20 (11.2 day)	03/17 16:00:12 (30 sec)
A dbw	- --	
A lgr	OK MH 03/06 11:10:20 (11.2 day)	03/17 16:00:17 (25 sec)
A rcv	OK 03/06 11:10:20 (11.2 day)	
A rtr	OK MH 03/06 11:10:20 (11.2 day)	03/17 16:00:15 (27 sec)
A rts	OK MH 03/06 11:10:20 (11.2 day)	03/17 16:00:19 (23 sec)
A tsyr	OK 03/06 11:10:20 (11.2 day)	
B agi	- --	
B cic	- --	
B csfs	OK 03/11 11:08:34 (6.2 day)	
B dba	OK MH 03/11 11:07:02 (6.2 day)	03/17 16:00:38 (4 sec)
B dbw	- --	
B lgr	OK MH 03/11 11:08:36 (6.2 day)	03/17 16:00:17 (25 sec)
B rcv	OK 03/11 11:08:35 (6.2 day)	

Process:	LastStateChange:	LastHeartBeat:
B rtr	OK MH 03/11 11:07:03 (6.2 day)	03/17 16:00:15 (27 sec)
B rts	OK MH 03/11 11:07:02 (6.2 day)	03/17 16:00:29 (13 sec)
B tsyr	OK 03/11 11:07:02 (6.2 day)	

First some general information is displayed such as Router version and build date. Then some statistics are displayed:

Current Time	This is Coordinated Universal Time (UTC). Most telecommunications equipment use UTC time as a common time reference.
Local Time	This is ICM local time, as determined by time zone setting on the Cisco ICM Call Router.
Router Up	This is how long the Cisco ICM Call Router function has been up and running.
Router Sync	This shows which side of the Cisco ICM call router last sent a state transfer to the other side.

Within the Status Process output, LastStateChange contains these fields:

OK	Signifies that the process is running fine.
M	Signifies the Cisco proprietary Message Delivery Service (MDS) protocol is used to keep the process synchronized.
H	Signifies that the process sends and receives internal heartbeat messages using the MDS protocol.
Date	Current date.
Time	Current local time.
Up-Time	In parenthesis is length of time the process has been in current state.
LastHeartBeat	If the process participates in sending and receiving MDS heartbeats, this value is the timestamp of the last heartbeat that was sent/received by the process.

Status Output: Controller

The second section, labeled Controller in the first column of the status output, shows the status of Cisco ICM peripheral gateway servers.

Controller is the name of the controller (ICM Peripheral Gateway) as defined in Configure initial cell rate (ICR).

Controller:	LastStateChange:	LastHeartBeat:
ATT_NIC_1,128	CFO 03/06 11:10:22 (11.2 day)	03/17 16:00:39 (3 sec)
ATT_NIC_2,129	CFO 03/11 11:07:05 (6.2 day)	03/17 16:00:34 (8 sec)
CA_PG9,9	CFO 03/17 04:42:31 (11.3 hr)	03/17 16:00:31 (11 sec)
FL_PG7,7	CFO 03/11 10:30:16 (6.2 day)	03/17 16:00:32 (10 sec)
GA_PG6,6	CFO 03/12 10:50:43 (5.2 day)	03/17 16:00:29 (13 sec)
IA_PG5,5	CFO 03/11 11:29:27 (6.1 day)	03/17 16:00:32 (10 sec)
NY_PG3,3	CFO 03/11 16:31:36 (5.9 day)	03/17 16:00:38 (4 sec)
TX_PG4,4	CFO 03/11 16:33:37 (5.9 day)	03/17 16:00:38 (4 sec)
VA_PG1,1	CFO 03/13 22:18:32 (3.7 day)	03/17 16:00:33 (9 sec)
VB_PG2,2	CFO 03/16 23:31:31 (16.4 hr)	03/17 16:00:32 (10 sec)

Within the Status Controller output, LastStateChange contains these fields:

C	Signifies that the ICM peripheral gateway server has successfully downloaded a configuration from the ICM call router.
F	Signifies that the ICM peripheral gateway is fully configured and the configuration is valid.
O	Signifies that the ICM peripheral gateway is online, and is communicating with the ICM call router.
Date	Current date.
Time	Current local time.

Up-Time	In parenthesis is length of time the process has been in current state.

Status Output: Peripheral

The third section labeled Peripheral in column 1, shows the status for third party peripherals such as ACD and VRU devices.

Peripheral is the name of the peripheral (ACD or VRU) as defined in Configure ICR.

Peripheral:	LastStateChange:	LastHeardFrom:
CA_PG9	COS 03/17 04:42:38 (11.3 hr)	03/17 16:00:40 (2 sec)
FL_PG7	COS 03/11 10:30:18 (6.2 day)	03/17 16:00:40 (2 sec)
GA_PG6	COS 03/16 06:21:18 (33.6 hr)	03/17 16:00:41 (1 sec)
IA_PG5	COS 03/11 11:29:30 (6.1 day)	03/17 16:00:40 (2 sec)
NY_PG3	COS 03/11 16:31:42 (5.9 day)	03/17 16:00:41 (1 sec)
TX_PG4	COS 03/11 16:37:53 (5.9 day)	03/17 16:00:34 (8 sec)
VA_PG1	COS 03/13 22:18:40 (3.7 day)	03/17 16:00:41 (1 sec)
VB_PG2	COS 03/16 23:31:33 (16.4 hr)	03/17 16:00:41 (1 sec)

Within the Status Peripheral output, LastStateChange contains these fields:

C	Signifies the peripheral is configured correctly to communicate with the ICM peripheral gateway.
O	Signifies the peripheral is online, for example, communications have been established with the ICM peripheral gateway.
S	Signifies that the peripheral is in service, for example, agent and call data are sent to the ICM peripheral gateway.
Date	Current date.
Time	Current local time.
Up-Time	In parenthesis is length of time the process has been in current state.

LastHeardFrom	Is the date, time, and length of time since the peripheral last sent valid data to the ICM peripheral gateway.

Parameter Descriptions

agent_status: Displays the states of agents and their groups.

agent_trace: Controls agent tracing in the router.

agi_lookup: Sends the router a application gateway lookup request.

checksum, check: Requests router to do a checksum.

cic_lookup: Sends the router a CIC lookup request.

cicr_time: Send ReportCICRTime message to the router.

closed_call: Sends a Closed call request to the router.

config: Enables config commands.

confignic: Sends a ConfigureNIC request to the router

configpd: Sends a ConfigurePD request to the router

configpg: Sends a ConfigurePG request to the router

configrc: Sends a ConfigureRC request to the router

db_lookup: Sends the router a db_lookup request.

db_meters: Displays meters about database accesses.

dbw_status: Display the dbworker status.

debug_control, debug: Controls various kinds of debugging output from router.

deconfig: Sends an message telling the router to de-configure.

dump: Requests router to do a internal state dump to a file.

dump_adminscript_info: Display Admin Script Information.

dump_adminscript_runtimes: Display Admin Script Run Times.

dump_call_types: Display the routers call type schedules.

dump_datain: Display the routers data input queue.

dump_hash: Display the routers internal hash statistics.

dump_indirect_route_meters: Display the routers indirect route meters.

dump_locks: Display the status of locks.

dump_region: Display the contents of a region.

dump_struct: Requests router to dump a structure.

dump_timers: Sends an message telling the router to display its timers.

dump_vars: Dumps info about router variables.

echo: Controls echoing of command lines

enable_config: Makes config commands visible.

error_stop: Controls setting of stop on error flag.

exit: Obsolete. Use exit_router or quit.

exit_dbw: Causes dbworker process to exit.

exit_router: Sends an message telling the router to exit.

expression, expr: Gives the router an expression to evaluate.

get_config: Causes the router to get config from logger.

help, ?: Displays this help.

mem_checkpoint: Controls SmartHeap checkpointing.

mem_meters: Displays router memory meters.

opi_data: Send OPI data message to the router.

quit, q: Ends the program.

read_file, read: Directs command input to another input file

rel_tranroute: Simulate PG releasing a translation route.

route_call: Sends a route call request to the router.

send_alarm: Forces the router to send a message as an alarm.

send_get_config: Sends a GetConfigInd request to the router

send_schedule: Sends a schedule to the router.

set_half_hour: Sends a SetHalfHour request to the router

startrc: Sends a StartRC request to the router

status: Sends an message telling the router to display its status.

stop_log: Requests logmsg to stop logging messages.

symbols: Displays names of objects and symbols.

test_edit_config: Causes router to load config with the scripted interface.

test_edit_script: Causes router to test the script real time data interface.

test_indirect_route: Test request for ScriptIndirectRoute.

test_route: Analyzes routes for valid labels.

test_update_script: Causes router to test the script update interface.

tuning_param, tune: Controls tuning in the router.

watch: Sends watch expressions to the router.

Turning up ICM Call Router Tracing with RTTest

You can enable specific trace levels within RTTest by issuing the debug command, followed by one or more trace options. Respective trace entries can then be viewed in router logs.

For example, debug /route turns up tracing to show:

- Dialed Number (DN)

- Automatic Number Identification (ANI)

- Caller Entered Digits (CED), if any

- ICM routing label returned to the carrier network.

To see all possibilities for /debug, at the RTTest prompt, enter **debug /?** as shown below.

```
rttest: debug /? Usage: debug_control [/realtime] [/5minute] [/agent]
[/config] [/route] [/halfhour] [/rcmeter] [/expr] [/select] [/dupadd]
[/failpgerror] [/symbol] [/tranroute] [/datain] [/delivery] [/cic] [/
admin] [/pervarsumm] [/pervardetail] [/expform] [/vru] [/callq] [/
activepath] [/all] [/help] [/?]
```

All ICM processes write some default level of tracing to log files that can be viewed with the Trace and Log utility.

- When specific trace levels are enabled, corresponding details are written to router log files in the logfile directory.

- Default individual log file size is 99k.

- Default aggregate log file size is 600k

- If router tracing is turned too high, individual log files will wrap very quickly, potentially within a minute if call volume is high. In that case, not much data can be captured because the time span is very small. To get around this, router log file capacities can be increased by altering a few Microsoft Windows registry settings. Make sure there is enough disk space available before increasing log file capacities.

  To enter the Windows registry:

  .a From a command prompt, enter regedt32.

  .b After checking available disk space, the following two registry settings can be changed to allow for larger router log files.

  Note: The values are displayed in hexadecimal by default. Click on the Decimal radio button to see the base 10 value.

  `\\.\software\geotel\icr\cisco\routera\ems\currentversion\library\processes\rtr\EMSAllLogFilesMax`

  `\\.\software\geotel\icr\cisco\routera\ems\currentversion\library\processes\rtr\EMSLogFileMax`

  The first parameter - **EMSAllLogFilesMax** specifies the maximum amount of disk space the router will allocate for all log files combined.

  The second parameter - **EMSLogFileMax** specifies the maximum size that the router will allocate to each log file. For example, if you set **EMSAllLogFilesMax** to 20 mg, and **EMSLogFileMax** to 2 mg, the router will eventually create no more than 10 files, each being no more than 2 mg in size.

Turning Off Debug Tracing in RTTest

When you are finished viewing router logs, it is good practice to disable all tracing that was added for troubleshooting purposes. Do this using the /noall directive as shown below:

```
c:\icm\cd\ra\logfiles>rttest /cust cd /node routera

rttest: debug /noall
```

Ending an RTTest Session

It is very important that you quit from your RTTest session when finished. If too many RTTest sessions are left running in the background, system resources will be drained and call routing will be adversely affected.

To quit an RTTest session, enter: `rttest: quit`

How to Use the SS7NICTrace Utility

Use SS7NICTrace to view and set debug trace bits on an ICM SS7 NIC PG.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Accessing SS7NICTrace

SS7NICTrace is an external GUI application present on all ICM nodes as part of that standard ICM installation. It cannot be run from within the Support Tools dashboard.

To access SS7NICTrace on an SS& NIC PG, from a command line, enter `ss7nictrace`.

How to Use the VRUTrace Utility

Use the VRUTrace utility to output tracing information from a Voice Response Unit (VRU) device, and to and from its PIM process. VRUTrace lets you capture and playback session data.

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

For use with ICM VRU PGs only.

To Access VRUTrace from the Dashboard

To run VRUTrace from the Support Tools Dashboard:

Step 1   Use the System Select screen to select the system you want to work with.

Step 2   From the Dashboard menu, select Cisco Common Tools > VRUTrace.

Step 3   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the `vrutrace` command is already implied. Do not enter it in the Arguments field.

Step 4   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 5   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 6   Click the Run button.

To Access VRUTrace from a Command Line on a Node

From a command-line on an ICM VRU PG, you must access VRUTrace from the `vrucap` directory located at: `<icm_root>\icm\<customer instance>\<pg#>`.

For example:

`c:\icm\my_customer_instance\pg1a\vrucap> vrutrace`

Using VRUTrace - Command Line Options

Syntax: `vrutrace [ProcessName] [/if InputFile] [/o] [/of OutputFile] [/bd BeginDate(mm/dd/yy)] [/bt BeginTime(hh:mm:ss)] [/ed EndDate(mm/dd/yy)] [/et EndTime(hh:mm:ss)] [/all] [/prev] [/last] [/binary] [/debug] [/sleep] [/htbt] [/vrustat] [/help] [/?]`

VRUTrace Examples

This example shows how you can obtain the output from a log file with information from April 29, 2003 until April 30, 2003 with binary data.

`c:\icm\xyz\pg1a\vrucap\vrutrace pim1 /bd 04/29/2003 /ed 04/30/2003 / binary`

This example shows how you can obtain output from a log file with information from the last time the process ran to the current date and time.

`c:\icm\xyz\pg1a\vrucap\vrutrace pim1 /last`

How to Use the VRUTrace Utility

Part 7: Using 3rd Party Common Tools

3rd Party Common Tools are a set of third-party utilities, present on all or most Windows/ICM systems, that may be useful when troubleshooting ICM components. For the sake of convenience, the Support Tools Dashboard provides direct access to these utilities through its interface.

Note: This guide does not provide detailed documentation on using third-party tools. In all cases, extensive documentation is available from a variety of sources, including user guides, the Web, and from the tools themselves. For those third-party utilities on which Cisco-specific documentation does exist on **http://www.cisco.com**, links have been provided.

These GUI-based third-party tools include:

- isql/w

- sqlew

- winmsd

Almost all 3rd Party Common Tools are installed on all Support Tools nodes/Windows OSs. Several (see the table in the next section) may be particular to SQL Server installations.

Most 3rd Party Common Tools are command-line based, and can be run from either the Support Tools Dashboard or from an individual node. Command-line access to individual nodes can be local or remote (via methods like TelNet, pcAnywhere, etc.).

Several 3rd Party Common Tools are GUI-based. While menu commands for these utilities appear in the Support Tools Dashboard, they cannot in fact be launched from there. Access to these tools is limited to the individual node (either locally or via remote GUI such as pcAnywhere).

Table 16: 3rd Party Common Tools At a Glance

Utility Name:	Description:	Supported Node Operating Systems:
Arp-a	Use to find the media access control address of a host on the same physical network.	Windows 2000, Windows 2003, Windows XP
cat	Use the CAT utility to display, print, and combine files. Equivalent of the DOS type command.	Windows 2000, Windows 2003, Windows XP
chmod	Use to change file permissions. Equivalent of the DOS attrib command.	Windows 2000, Windows 2003, Windows XP
cp	Equivalent of the DOS copy command.	Windows 2000, Windows 2003, Windows XP

Utility Name:	Description:	Supported Node Operating Systems:
df	Use to view disk free information.	Windows 2000, Windows 2003, Windows XP
diff	Use to compare two text files or two directories.	Windows 2000, Windows 2003, Windows XP
du	Use to view disk usage information.	Windows 2000, Windows 2003, Windows XP
fgrep	Use to search for text patterns within a set of files.	Windows 2000, Windows 2003, Windows XP
findstr	Use to find strings in logs or text files. Similar to UNIX's grep command. Useful when parsing log files or other text files to find a snippet of text.	Windows 2000, Windows 2003, Windows XP
grep	Use to search for text patterns within a set of files.	Windows 2000, Windows 2003, Windows XP
head	Use to view user-defined number of lines from the start of a file.	Windows 2000, Windows 2003, Windows XP
IPConfig -all	Use to get host computer configuration information, including the IP address, subnet mask, and default gateway.	Windows 2000, Windows 2003, Windows XP
isql/w	Interactive SQL for Windows. Use to query and update Microsoft SQL Server databases.	Windows 2000, Windows 2003, Windows XP
ls	Use to view directory listings. Equivalent of the DOS dir command.	Windows 2000, Windows 2003, Windows XP
mv	Use to move files and directories. Equivalent of the DOS move or rename command.	Windows 2000, Windows 2003, Windows XP
NBTStat	Use to troubleshoot NetBIOS name resolution problems.	Windows 2000, Windows 2003, Windows XP
Net Session	Use to view information about all current client sessions with the current system.	Windows 2000, Windows 2003, Windows XP
NetStat	Use to view network information for the current system, including protocol statistics and current TCP/IP network connections.	Windows 2000, Windows 2003, Windows XP

Utility Name:	Description:	Supported Node Operating Systems:
Net Statistics Server	Use to view statistics for the local Server service.	Windows 2000, Windows 2003, Windows XP
Net Statistics Works	Use to view statistics for the local Workstation service.	Windows 2000, Windows 2003, Windows XP
NSLookup	Use to get the IP address and fully qualified DNS of the current system's DNS name server.	Windows 2000, Windows 2003, Windows XP
PathPing	A route tracing tool that combines features of the ping and tracert commands with additional information.	Windows 2000, Windows 2003, Windows XP
ping	Low-level connectivity test. Use to verify end-to-end TCP/IP network infrastructure.	Windows 2000, Windows 2003, Windows XP
pstat	Use to list all NT or Win2K processes, their process ID (PID), memory and cpu utilization, etc.	Windows 2000, Windows 2003, Windows XP
rm	Use to delete files and directories. Equivalent of the DOS delete, recursive del subdirectories commands.	Windows 2000, Windows 2003, Windows XP
Route-print	Use to view the contents of the network routing tables.	Windows 2000, Windows 2003, Windows XP
shutdown	Use to shut down a remote host. When used from the Dashboard, shutdown will automatically restart the host after 60 seconds.	Windows 2000, Windows 2003, Windows XP
sqlew	SQL Enterprise Manager. Use to monitor and update SQL Server operating parameters, expand databases, etc.	Windows 2000, Windows 2003, Windows XP
stopshut	Use to stop a system from shutting down due to an application or operating system failure.	Windows 2000, Windows 2003, Windows XP
strings	Use to find printable strings in a binary file.	Windows 2000, Windows 2003, Windows XP
tail	Use to view user-defined number of lines from end of a file.	Windows 2000, Windows 2003, Windows XP
touch	Use to change the creation date/time for any file.	Windows 2000, Windows 2003, Windows XP

Utility Name:	Description:	Supported Node Operating Systems:
tracert	Related to ping command. Use to show each intermediary Hop in the TCP/IP network. Useful in troubleshooting LAN and WAN faults.	Windows 2000, Windows 2003, Windows XP
wc	Use to view a count of characters, words, or lines in a file.	Windows 2000, Windows 2003, Windows XP
which	Use to view the name of the first file encountered while traversing a path or directory tree.	Windows 2000, Windows 2003, Windows XP
winmsd	Windows Diagnostics. Use to gather detailed configuration information about computers running Windows.	Windows 2000, Windows 2003, Windows XP
NetshDump	Allows you to run the NetShell utility to display or modify the configuration of a currently running computer.	Windows 2000, Windows 2003, Windows XP
Bootcfgqry	Queries Boot.ini file settings.	Windows 2003, Windows XP
Defraganalyze	Analyzes boot files, data files, and folders on local volumes for fragmentation.	Windows 2003, Windows XP
Defragreport	Reports fragmentation of boot files, data files, and folders on local volumes.	Windows 2003, Windows XP
Driverquery	Displays a list of all installed device drivers and their properties.	Windows 2003, Windows XP
Eventtriggers	Displays and configures event triggers on local or remote machines.	Windows 2003, Windows XP
Getmac	Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.	Windows 2003, Windows XP
Logman	Manages and schedules performance counter and event trace log collections on local and remote systems.	Windows 2003, Windows XP
Openfiles	Queries or displays open files. Also queries, displays, or disconnects files opened by network users.	Windows 2003, Windows XP
Relog	Extracts performance counters from performance counter logs into other formats, such as text-TSV (for tab-delimited text), text-CSV (for comma-delimited text), binary-BIN, or SQL.	Windows 2003, Windows XP

Utility Name:	Description:	Supported Node Operating Systems:
SC	Communicates with the Service Controller and installed services. SC.exe retrieves and sets control information about services.	Windows 2003, Windows XP
Schtasks	Schedules commands and programs to run periodically or at a specific time. Adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.	Windows 2003, Windows XP
SysteminfoTable	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	Windows 2003, Windows XP
SysteminfoList	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	Windows 2003, Windows XP
SysteminfoCSV	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.	Windows 2003, Windows XP
Taskkill	Ends one or more tasks or processes. Processes can be killed by process ID or image name.	Windows 2003, Windows XP
TasklistTable	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	Windows 2003, Windows XP
Tasklist	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	Windows 2003, Windows XP
TasklistCSV	Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.	Windows 2003, Windows XP

Chapter 14

Using 3rd Party Common Tools

Arp -a

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

The Address Resolution Protocol (Arp) allows a host to find the media access control address of a host on the same physical network, given the IP address of the host. To make ARP efficient, each computer caches IPÃƒâ€šÃ‚toÃƒâ€šÃ‚media access control address mappings to eliminate repetitive Arp broadcast requests.

You can use the **arp -a** command to view the Arp table entries on a specified host. The arp command is useful for viewing the Arp cache and resolving address resolution problems.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Options for this tool:

1. **Command duration (seconds)** - Enter the max execution time for this command.

2. **Elevate command priority on remote system** - Cause command to run at a higher priority.

cat

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the CAT utility to display, print, and combine files.

To Access CAT from the Dashboard

To run CAT from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using CAT - Command Line Options

cat [-usx?] [-v [-t] [-e]] file1 ...

The options for CAT are:

-u: output characters one at a time, not a line at a time.

-s: be silent about non-existent files.

-v: visible mode - display control characters as ^<char> (except for tabs, new-lines, and form-feeds) and chars with the 8th bit set as M-<char>.

-t: show tabs as ^I (only valid if -v given).

-e: show new-lines as $ (only valid if -v given).

-x: expand tabs into the number of spaces specified by the TABS environment variable or into 8 spaces if TABS is undefined.

-n: no output - don't actually do any output, just do input. Equivalent to '> null', except that on some platforms, the latter can be very slow (much slower than writing to an actual file.) This option is handy for seeing how long it takes to just read a set of files under varying operating conditions.

-?: Display program description.

Note: If the environment variable CAT exists, its value is used to establish default options.

You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -v option, specify -v-.

If the environment variable TABS exists, its value will determine the number of spaces used to expand tabs. Otherwise, tabs are expanded to 8 spaces.

chmod

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the CHMOD utility to set file permissions.

To Access CHMOD from the Dashboard

To run CHMOD from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

When entering arguments, the CHMOD command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using CHMOD - Command Line Options

```
chmod <mode> file1 ...
```

Mode is any combination of {+|-|=} {w|s|h|m} where:

+ adds an attribute to a file

- removes an attribute from a file

= gives a file just the attributes specified

w specifies whether the file should be writable or not

s specifies whether the file should be a system file or not

h specifies whether the file should be a hidden file or not

m specifies whether the file should be marked modified or not

-?: Display program description.

Note: If the environment variable CHMOD exists, its value is used to establish default options.

cp

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the CP utility to copy files.

To Access CP from the Dashboard

To run CP from the Support Tools Dashboard:

Step 1	In the Arguments field, enter desired arguments, as described in the Using section below.
	Note: When entering arguments, the CP command is already implied. Do not enter it in the Arguments field.
Step 2	Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.
Step 3	If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.
Step 4	Click the Run button.

Using CP - Command Line Options

```
cp [-ifprv?] file1 file2

cp [-ifprvd?] file1 fileN directory
```

If the last file is a directory, each file is copied into a file in the destination directory with the same name.

If only two files are specified, file1 is copied to file2.

If more than two files are specified, the last file must be a directory.

The options for CP are:

-i: ask for confirmation before overwriting each destination file.

-f: copy the file, don't ask for confirmation even if it will overwrite a file marked Read-Only.

-p: preserve the source attributes and last modified date and time for the destination file. This is the default. To turn if off use -p-.

-r: recursively copy all of the files and subdirectories specified by the filename, including the named directory.

-v: print out status as the cp progresses.

-d: preserve the directory structure of the specified files (which must all be specified with relative paths) when placing them in the specified directory. For example, 'cp -d foo\bar\baz otherdir' will make the directories otherdir\foo and otherdir\bar if necessary, then copy foo\bar\baz to otherdir\foo\bar\baz.

-?: Display program description.

Note:

- If the environment variable CP exists, its value is used to establish default options.

- You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -I option, specify -I-.

- The order of options f and I is significant: the one specified last determines whether a confirmation is requested.

df

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the DF utility to view information on file system disk space usage.

To Access DF from the Dashboard

To run DF from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the DF command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using DF - Command Line Options

```
df [ -a | drive_1 [ drive_2 ... ] | -? ]
```

If DF is not given an argument, it will print the free space information for the default drive. Otherwise, unless the -a option is specified, DF prints the free space information for each of the supplied arguments.

Example: **df a: b:** prints the available free space for drives a: and b:.

The options for DF are:

-a: Print free space for all loadable drives.

-?: Display program description.

Note:

- If the environment variable DF exists, its value is used to establish default options.

- You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -a option, specify -a-.

- Option -a can be specified twice to restore normal operation, namely, to undo the effect of specifying option -a in the environment variable.

diff

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Diff utility to find differences between two text files.

To Access Diff from the Dashboard

To run Diff from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Diff command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Diff - Command Line Options

`diff [ -rebidtvo? ] [-O <colors>] oldfile newfile`

If diff is given two directories, it will diff each of the files in those directories.

If diff is given two binary files, it will compare them and issue a report if they are different.

If diff is given the -r option, it will recursively diff each of the files in each subdirectory.

If diff is given the -e option, it will output a script suitable for feeding into EDLIN to update oldfile to create newfile.

Otherwise, diff outputs lines of the form:

`n1 a n3,n4`

`n1,n2 d n3`

`n1,n2 c n3,n4`

where 'a' means: add lines n3 thru n4 from newfile at location n1 in newfile; 'd' means: delete lines n1 thru n2 from newfile, next line is n3 in newfile; and 'c' means: change lines n1 thru n2 in newfile to lines n3 thru n4 in newfile Identical pairs where n1=n2 or n3=n4 are abbreviated as a single number. Following each of the [adc] lines comes each of the lines effected. Lines preceded by '<' are from oldfile, those preceded by '>' are from newfile.

The options for Diff are:

-b: Ignore trailing whitespace and treat sequences of embedded whitespace as being equal.

-i: Ignore leading whitespace.

-d: Treat files as if they were binary, only reporting if they are different.

-t: Treat files as if they were text, even if default autodetection claims they are binary.

-v: Report on each file that it processes, not just the ones with differences.

-o: Colorize output with the default colors (black, white, light cyan, and yellow), just as '-O 0fbe' would.

-O <colors>: Colorize output with the specified single-character hex colors: background, normal text, old text, and new text. The colors are: black = 0, blue = 1, green = 2, cyan = 3, red = 4, magenta = 5, brown = 6, lightgray = 7, darkgray = 8, lightblue = 9, lightgreen = A, lightcyan = B, lightred = C, lightmagenta = D, yellow = E, white = F.

-?: Display program description.

Note:

• If the environment variable DIFF exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -b option, specify -b-.

du

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the DU utility to view the sizes of each directory specified on the command line and the sizes of each subdirectory under those.

To Access DU from the Dashboard

To run DU from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the DU command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using DU - Command Line Options

```
du [ -asM? ] [ names ]
```

If no names are specified on the command line, the size of the current directory is given. Sizes given show the total number of bytes in all of the files within and below the named directory and the amount of disk space used by the files in and below the named directory. The disk space is displayed in Kbytes (1024 bytes = 1 Kbyte)

The options for DU are:

-a: also display the size of each file.

-s: only display the grand totals for the names on the command line.

-M: show file names in their OS-provided mixed-case forms, rather than lower-casing them. Note however that most file systems don't allow files with names differing only by case, and will ignore case differences when looking for a file.

-?: Display program description.

Note:

- If the environment variable DU exists, its value is used to establish default options.

- You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -a option, specify -a-.

fgrep

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the FGrep utility to perform a fast search for text patterns through text files.

To Access FGrep from the Dashboard

To run FGrep from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the FGrep command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using FGrep - Command Line Options

```
fgrep [ -mvclxinfse? ] <pattern> file1 ...
```

If no names are specified on the command line, the size of the current directory is given. Sizes given show the total number of bytes in all of the files within and below the named directory and the amount of disk space used by the files in and below the named directory. The disk space is displayed in Kbytes (1024 bytes = 1 Kbyte)

The options for FGrep are:

-m: print the lines that match the pattern (DEFAULT).

-v: print the lines that DON'T match the pattern.

-c: print a count of the number of matching lines in each file.

-l: print the name of each file that has a match.

Note: Options m, v, c and l are exclusive. Only one of these may be selected.

-x: the pattern must match the entire line to succeed.

-i: ignore the case of each character while matching.

-n: print the line number that the match occurred on.

-f: print the full path name of the file when printing filenames.

-s: do not report errors encountered while opening or reading files.

-e: use the next argument as the pattern to search for. This is useful if the pattern begins with a - or / character.

-?: Display program description.

Note: If the environment variable FGrep exists, its value is used to establish default options.

You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -I option, specify -I-.

FindStr

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Findstr utility to find strings in logs or text files. Findstr is useful when parsing log files or other text files for a snippet of text.

To Access Findstr from the Dashboard

To run Findstr from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Findstr command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Findstr - Command Line Options

```
FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P]
[/F:file] [/C:string] [/G:file] [/D:dir list] [/A:color attributes]
[strings] [[drive:][path]filename[ ...]]
```

If no names are specified on the command line, the size of the current directory is given. Sizes given show the total number of bytes in all of the files within and below the named directory and the amount of disk space used by the files in and below the named directory. The disk space is displayed in Kbytes (1024 bytes = 1 Kbyte)

The options for Findstr are:

/B: Matches pattern if at the beginning of a line.

/E: Matches pattern if at the end of a line.

/L: Uses search strings literally.

/R: Uses search strings as regular expressions.

/S: Searches for matching files in the current directory and all subdirectories.

/I: Specifies that the search is not to be case-sensitive.

/X: Prints lines that match exactly.

/V: Prints only lines that do not contain a match.

/N: Prints the line number before each line that matches.

/M: Prints only the filename if a file contains a match.

/O: Prints character offset before each matching line.

/P: Skip files with non-printable characters

/A:attr: Specifies color attribute with two hex digits. See "color /?"

/F:file: Reads file list from the specified file (/ stands for console).

/C:string: Uses specified string as a literal search string.

/G:file: Gets search strings from the specified file (/ stands for console).

/D:dir: Search a semicolon delimited list of directories

strings: Text to be searched for.

[drive:][path]filename: Specifies a file or files to search.

-?: Display program description.

Use spaces to separate multiple search strings unless the argument is prefixed with /C. For example, 'FINDSTR "hello there" x.y' searches for "hello" or "there" in file x.y. 'FINDSTR /C:"hello there" x.y' searches for "hello there" in file x.y.

Regular expression reference:

- **.** Wildcard: any character

- ***** Repeat: zero or more occurrence of previous character or class

- **^** Line position: beginning of line

- **$** Line position: end of line

- **[class]** Character class: any one character in set

- **[^class]** Inverse class: any one character not in set

- **[x-y]** Range: any characters within the specified range

- **\x** Escape: literal use of metacharacter x

- **\<xyz** Word position: beginning of word

- **xyz\>** Word position: end of word

grep

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Grep utility to perform a regular expression search for text patterns through text files.

To Access Grep from the Dashboard

To run Grep from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Grep command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Grep - Command Line Options

`grep [ -mvclinfse? ] <pattern> file1 ...`

The options for Grep are:

-m: print the lines that match the pattern (DEFAULT).

-v: print the lines that DON'T match the pattern.

-c: print a count of the number of matching lines in each file.

-l: print the name of each file that has a match.

Note: Options m, v, c and l are exclusive. Only one of these may be selected.

-i: ignore the case of each character while matching.

-n: print the line number that the match occurred on.

-f: print the full pathname of the file when printing filenames.

-s: do not report errors encountered while opening or reading files.

-e: use the next argument as the pattern to search for. This is useful if the pattern begins with a - or / character.

-?: Display program description.

The specified pattern is treated as a regular expression -- if all you need is a literal expression, you may want to use fgrep instead. The actual regular expression syntax is fairly standard, but escape sequence issues can complicate it. Here's an example of the 'pristine' syntax seen internally:

`^a.b+c*(d|e)?[^f]\*"$`

means "in beginning-of-line context, match 'a', then an arbitrary character, then one or more 'b's, then zero or more 'c's, then one of 'd', 'e', or nothing, then any character but 'f', then a literal '*' character, then a double-quote character, in end-of-line context."

The first added complication is the Picnix command-line argument parser, which has special semantics for ", ', `, @, $, and ^. So the argument as seen by this parser would have to be:

```
^^a.b+c*(d|e)?[^^f]\*^"$
```

The second added complication is that you may be executing grep through an additional shell, such as the WinNT cmd.exe, which has special semantics for |, ^, ", and \, and for which you should actually put this on the command line or in your batch file:

```
"^^a.b+c*(d|e)?[^^f]\*^"$"
```

Or you may be executing grep through a build tool like pmake.exe, for which you'd have to say:

```
"^^^^a.b+c*(d|e)?[^^^^f]\*^^"$$"
```

Note:

- If the environment variable Grep exists, its value is used to establish default options.

- You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -I option, specify -I-.

head

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Head utility to view a user-defined number of lines from the start of a file.

To Access Head from the Dashboard

To run Head from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Head command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Head - Command Line Options

Head displays the first <count> lines of each of the files listed on the line. If no files are listed, display the first <count> lines of the standard input.

<count> defaults to 10.

head [-<count> | -n <count>] [-vx?] [file1 ...]

The options for Head are:

-<count> or -n <count>: specifies the number of lines to display.

-v: Print headers giving file names.

-x: Expand tabs into the number of spaces specified by the TABS environment variable or into 8 spaces if TABS is undefined.

-?: Display program description.

Note:

• If the environment variable Head exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -v option, specify -v-.

• If the environment variable TABS exists, its value will determine the number of spaces used to expand tabs. Otherwise, tabs are expanded to 8 spaces.

IPConfig /all

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

When you troubleshoot a TCP/IP networking problem, begin by checking the TCP/IP configuration on the computer that is experiencing the problem.

Use the IPConfig -all command to get host computer configuration information, including the IP address, subnet mask, and default gateway. When you use the IPConfig command with the -all option, a detailed configuration report is produced for all interfaces, including any configured serial ports.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

ISQL

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

ISQL is an application used to query and update Microsoft SQL Server databases.

To Access ISQL from the Dashboard

To run ISQL from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using ISQL

ISQL uses the following options:

- **[-U login id]**

- **[-P password]**

- **[-S server]**

- **[-H hostname]**

- **[-E trusted connection]**

- **[-d use database name]**

- **[-l login timeout]**

- **[-t query timeout]**

- **[-h headers]**

- **[-s colseparator]**

- **[-w columnwidth]**

- **[-a packetsize]**

- **[-e echo input]**

- **[-x max text size]**

- **[-L list servers]**

- **[-c cmdend]**

- **[-q "cmdline query"]**

- **[-Q "cmdline query" and exit]**

- **[-n remove numbering]**

- **[-m errorlevel]**

- **[-r msgs to stderr]**

- **[-I inputfile]**

- **[-o outputfile]**

- **[-p print statistics]**

- **`[-b On error batch abort]`**

- **`[-O use Old ISQL behavior disables the following] <EOF> batch processing Auto console width scaling Wide messages default errorlevel is -1 vs 1`**

- **`[-? show syntax summary (this screen)]`**

ISQLW

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the ISQL/W utility to query and update Microsoft SQL Server databases.

Accessing ISQL/W

ISQL/W is a Microsoft external GUI application present on systems with Microsoft SQL Server installed. It cannot be run from within the Support Tools dashboard.

To access ISQL/W:

Step 1   On the Windows Start bar, click Start > Run.

Step 2   In the Open field, enter **`isqlw`**.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click OK.

---

ls

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the LS utility to view directory listings.

To Access LS from the Dashboard

To run LS from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using LS - Command Line Options

`ls [ -cx1lmfetsurRpadoM? ] [ file1 ... ]`

The options for LS are:

-c: display the names of the files sorted down each column.

-x: display the names of the files sorted across the row.

-1: display the names of the files in a single column.

-l: display a long listing with more information about each file.

-m: display the names of the files separated by commas.

-f: sort the files by filename.

-e: sort the files first by the extension and then by the filename.

-t: sort the files by the date and time that the files were last written.

-s: sort the files by the size (in bytes).

-u: do not sort the files.

-r: reverse the order of the sort selected.

-R: recursively descend down each subdirectory.

-p: put a slash (/ or \) after each directory.

-a: list all files, including HIDDEN files.

-d: when a directory is specified on the command line, display it as an individual item rather than displaying its contents.

-o: when a high-bit (greater than 127) character in a filename is displayed, assume the name is in the Windows/ANSI character set and convert it to the DOS/OEM character set, just like 'dir' does. This means that for commonly-used accent characters in Windows filenames, they'll look the same in a OEM character-set-based command prompt. Note however that this may result in output which obscures actual distinctions, since the conversion is not always reversible. For

example, four accented Windows/ANSI versions of 'A' (0xc0 - 0xc4) all map to 'A' under this conversion. Also note that ls will only ever show single-byte filenames, even if the underlying file system has Unicode filenames -- when dealing with a file with Unicode characters in its name, the Picnix utilities will try to use the OS-provided 8.3 short filename instead.

-M: show file names in their OS-provided mixed-case forms, rather than lower-casing them. Note however that most file systems don't allow files with names differing only by case, and will ignore case differences when looking for a file.

-?: Display program description.

Note:

• If the environment variable LS exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -p option, specify -p-.

mv

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the MV utility to move files and directories.

To Access MV from the Dashboard

To run MV from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the MV command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using MV - Command Line Options

```
mv [-firv?] file1 file2

mv [-firv?] file1 ... fileN directory
```

If the last file is a directory, each file is moved into a file in the destination directory with the same name.

If only two files are specified, file1 is moved to file2.

If more than two files are specified, the last file must be a directory.

The options for MV are:

-i: ask for confirmation before overwriting each destination file.

-f: move the file, don't ask for confirmation even if it will overwrite a file marked Read-Only.

-r: recursively move all of the files and subdirectories specified by the filename, including the named directory.

-v: print out status as the mv progresses.

-?: Display program description.

Note:

• If the environment variable MV exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -I option, specify -I-.

• The order of options f and I is significant: the one specified last determines whether a confirmation is requested.

• If the environment variable MV exists, its value is used to establish default options.

NBTStat

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the NBTStat utility to troubleshoot NetBIOS name resolution problems. NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. TCP/IP provides many options for NetBIOS name resolution, including local cache lookup, WINS server query, broadcast, DNS server query, and Lmhosts and Hosts file lookup.

To Access NBTStat from the Dashboard

To run NBTStat from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using NBTStat - Command Line Options

```
nbtstat [ [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [interval] ]
```

The options for NBTStat are:

-a (adapter status) Lists the remote machine's name table given its name

-A (Adapter status) Lists the remote machine's name table given its IP address.

-c (cache) Lists NBT's cache of remote [machine] names and their IP addresses

-n (names) Lists local NetBIOS names.

-r (resolved) Lists names resolved by broadcast and via WINS

-R (Reload) Purges and reloads the remote cache name table

-S (Sessions) Lists sessions table with the destination IP addresses

-s (sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names.

-RR (ReleaseRefresh) Sends Name Release packets to WINs and then, starts Refresh

RemoteName Remote host machine name.

IP address Dotted decimal representation of the IP address.

interval Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

Net Session

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Net Session utility to view information about all current client sessions with the current system. Net Session displays the computer names and user names of users on a server, to see if users have files open, and to see how long each user's session has been idle.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Net Statistics Server

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Net Statistics Works utility to view statistics for the local Server service.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Net Statistics Workstation

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Net Statistics Workstation utility to view statistics for the local Workstation service.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

NetStat

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the NetStat utility to view network information for the target host, including protocol statistics and current TCP/IP network connections.

To Access NetStat from the Dashboard

To run NetStat from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the NetStat command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using NetStat - Command Line Options

```
NetStat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

The options for NetStat are:

-a Displays all connections and listening ports.

-e Displays Ethernet statistics. This may be combined with the -s option.

-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

-?: Display program description.

NSLookUp

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the NSLookup utility to get information on the current or specified system's DNS name server.

To Access NSLookup from the Dashboard

To run NSLookup from the Support Tools Dashboard:

Step 1   enter the IP address or DNS of the system you want to query--OR--to get DNS name server information for the current system, leave the Arguments field blank.

Note: When entering arguments, the NetStat command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using NSLookup - Command Line Options

nslookup ip_address or hostname

Example: **nslookup www.cisco.com**

PathPing

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the PathPing utility as a route tracing tool that combines features of the Ping and Tracert utilities with additional information that neither of those tools provides (for example QOS testing).

To Access PathPing from the Dashboard

To run PathPing from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the strings command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using PathPing - Command Line Options

pathping [-n] [-h maximum_hops] [-g host-list] [-p period] [-q num_queries] [-w timeout] [-t] [-R] [-r] target_name

The options for PathPing are:

-n: Do not resolve addresses to hostnames.

-h maximum_hops: Maximum number of hops to search for target.

-g host-list: Loose source route along host-list.

-p period: Wait period milliseconds between pings.

-w timeout: Wait timeout milliseconds for each reply.

-T: Test connectivity to each hop with Layer-2 priority tags.

-R: Test if each hop is RSVP aware.

Ping

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Ping utility to verify IP-level connectivity. When troubleshooting, you can use Ping to send an ICMP echo request to a target host name or IP address. Use Ping whenever you need to verify that a host computer can connect to the TCP/IP network and network resources. You can also use Ping to isolate network hardware problems and incompatible configurations.

To Access Ping from the Dashboard

To run Ping from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Ping - Command Line Options

```
ping [-t] [-a] [-n count] [-l size] [-f] [-I TTL] [-v TOS] [-r count]
[-s count] [[-j host-list] | [-k host-list]][-w timeout]
destination-list
```

The options for Ping are:

-t: Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.

-a: Resolve addresses to hostnames.

-n count: Number of echo requests to send.

-l sizeSend: buffer size.

-f Set: Don't Fragment flag in packet.

-I TTL: Time To Live.

-v TOS: Type Of Service.

-r count: Record route for count hops.

-s count: Timestamp for count hops.

-j host-list: Loose source route along host-list.

-k host-list: Strict source route along host-list.

-w timeout: Timeout in milliseconds to wait for each reply.

PStat

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the PStat utility to list all the processes running on a Microsoft Windows Workstation, including ICM processes. You can use the PStat command to verify that an ICM process was not properly exited and is still running.

Note:

• You can also achieve this using the Support Tools Processes utility.

• Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

rm

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the RM utility to delete files and directories.

To Access RM from the Dashboard

To run RM from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the RM command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using RM - Command Line Options

```
rm [ -firv? ] file ...
```

The options for RM are:

-i: ask for confirmation before removing each file.

-f: remove the file, don't ask for confirmation even if it is marked Read-Only.

-r: recursively delete all of the files and subdirectories specified by the filename, including the named directory.

-v: print out the name of each file that is removed.

-?: Display program description.

Note:

• If the environment variable RM exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -I option, specify -I-.

Route -PRINT

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Route -print utility to view the contents of the network routing tables.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Shutdown Tool

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Shutdown Tool utility to stop and restart a remote host after a 60 second grace period.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

StopShut

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Stopshut utility to stop a system from shutting down due to an application or operating system failure.

To Access Stopshut from the Dashboard

To run Stopshut from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the stopshut command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using Stopshut - Command Line Options

```
c:\>stopshut
```

SQLEW

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the SQLEW utility to monitor and update SQL Server operating parameters, expand databases, and so on.

Accessing SQLEW

SQLEW is a Microsoft external GUI application present on all Windows 2000 installations. It cannot be run from within the Support Tools dashboard.

To access SQLEW:

Step 1   On the Windows Start bar, click Start > Run.

Step 2   In the Open field, enter sqlew.

Step 3   Click OK.

Strings

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Strings utility to print ASCII strings embedded in binary files.

To Access Strings from the Dashboard

To run Strings from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the strings command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Strings - Command Line Options

Strings displays printable ASCII strings in the binary files specified on the command line. If no files are given, it displays printable ASCII strings in the standard input.

strings [-?] [-t <n>] [-n <n>] [file1 ...]

The options for strings are:

-t <n>: specifies the minimum length that a terminated string needs to be before it is printed (default 4).

-n <n>: specifies the minimum length that a non-terminated string needs to be before it is printed (default 8).

-?: Display program description.

Note: If the environment variable STRINGS exists, its value is used to establish default options.

tail

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Tail utility to view user-defined number of lines from end of a file.

To Access Tail from the Dashboard

To run Tail from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Tail command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using Tail - Command Line Options

Tail displays the last <count> lines of each of the files listed on the line. If no files are listed, display the last <count> lines of the standard input.

<count> defaults to 10.

tail [-<count> | -n <count>] [-fvx?] [file1 ...]

The options for Tail are:

-<count> or -n <count>: specifies the number of lines to display.

-f: Follow along forever, outputting appended data as the file grows.

-v: Print headers giving file names.

-x: Expand tabs into the number of spaces specified by the TABS environment variable or into 8 spaces if TABS is undefined.

-?: Display program description.

Note:

• If the environment variable TAIL exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -v option, specify -v-.

• If the environment variable TABS exists, its value will determine the number of spaces used to expand tabs. Otherwise, tabs are expanded to 8 spaces.

touch

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Touch utility to change the creation date/time for any file.

To Access Touch from the Dashboard

To run Touch from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Touch command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Touch - Command Line Options

Touch displays the last <count> lines of each of the files listed on the line. If no files are listed, display the last <count> lines of the standard input.

<count> defaults to 10.

```
touch [ -c? ] [ mmddhhmm[yy] ] file1 ...
```

The options for Touch are:

-c: Prevents touch from creating files that did not previously exist

If an argument in the form mmddhhmm[yy] is passed to touch, the last-write time of each file listed on the command line is set to the specified date and time. If the date and time are not given on the command line, the last-write times of the arguments are set to the current system time. The argument mmddhhmm[yy] is formed as follows:

- The first mm is a two digit number (between 01 and 12) for the month.

- The dd is a two digit number (between 01 and 31) for the day of the month.

- The hh is a two digit number (between 00 and 23) for the hour. Note that a 24 hour clock is assumed.

- The second mm is a two digit number (between 00 and 59) for the minute.

- The yy, if present, is for setting the year. Years between 80 and 99 are understood to be between 1980 and 1999. Years between 00 and 79 are assumed to be for the years 2000 to 2079.

-?: Display program description.

Note: If the environment variable TOUCH exists, its value is used to establish default options.

You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -v option, specify -v-.

Tracert

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Tracert (Trace Route) is a route-tracing utility that is used to determine the path that an IP datagram takes to reach a destination. The tracert command uses the IP Time-to-Live (TTL) field and ICMP error messages to determine the route from one host to another through a network.

To Access Tracert from the Dashboard

To run Tracert from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the tracert command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Tracert - Command Line Options

`tracert ip_address or hostname`

Example: **`tracert www.cisco.com`**

WC

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the WC utility to view a count of characters, words, or lines in a file.

To Access WC from the Dashboard

To run WC from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the wc command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using WC - Command Line Options

```
wc [ -lwc? ] [ file1 ... ]
```

The default is for wc to count lines, words, and characters for each file given. Counting can be restricted to one or more of lines, words, or characters by using the command line options below:

-l: Enable counting for lines.

-w: Enable counting for words.

-c: Enable counting for characters.

If no files are given, standard input is read for characters.

-?: Display program description.

Note: If the environment variable WC exists, its value is used to establish default options.

which

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the Which utility to view the name of the first file encountered while traversing a path or directory tree.

To Access Which from the Dashboard

To run Which from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the which command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Which - Command Line Options

```
which [ -a? ] [ -p <environment variable> ] file1 ...
```

Which will print the full pathname of the first occurrence of a file found in the current directory or along a given path. The default path is the value of the environment variable PATH. If the filename does not have an extension, which will print the first occurrence of <file>.com, <file>.exe, <file>.bat, or <file>.cmd, in that order (unless the environment variable PATHEXT is set, in which case its list of extensions is used.)

-a: Prints the full pathnames of all of the files found along the specified path. Note that if the path specifies the same directory more than once (which may include the implicit current directory), the same pathname may occur more than once.

-p: Use the next argument as the name of the environment variable whose value contains the path to search and will not automatically add the extension as described above.

-?: Display program description.

Note:

• If the environment variable WHICH exists, its value is used to establish default options.

• You can override an option that was specified in the environment variable by following the option with a minus '-' sign. For example, to turn off the -a option, specify -a-.

Winmsd

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Use the WinMSD utility to view and generate reports that capture detailed Windows system configuration information.

Accessing WinMSD

WinMSD is a Microsoft external GUI application present on all Windows 2000 installations. It cannot be run from within the Support Tools dashboard.

Step 1   On the Windows Start bar, click Start > Run.

Step 2   In the Open field, enter `winmsd`.

Step 3   Click OK

NetshDump

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Netsh is a command-line scripting utility that allows you to, either locally or remotely, display the network configuration of a computer that is currently running.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Bootcfgqry

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays the Boot.ini file settings of the selected system..

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Defraganalyze

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Analyzes the volumes (hard drives) on the selected system and determines whether or not a defrag is recommended for any system volumes.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Defragreport

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays a volume (hard drive) fragmentation report for the hard drives on the selected system.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Driverquery

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays a list of all installed device drivers and their properties.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Eventtriggers

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

This tool enables an administrator to display and configure "Event Triggers" on local or remote systems.

To Access Eventtriggers from the Dashboard

To run Eventtriggers from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Eventtriggers command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3 If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4 Click the Run button.

Using Eventtriggers - Command Line Options

EVENTTRIGGERS /parameter [arguments]

The options for Eventtriggers are:

/Create: Create a new Event Trigger.

/Delete: Deletes an Event Trigger by its trigger ID.

/Query: Displays the Event Trigger properties and settings.

/?: Displays help/usage.

Examples (Addition Command Line Option help is provided in the tool by using the following examples):

EVENTTRIGGERS /Create /?

EVENTTRIGGERS /Delete /?

EVENTTRIGGERS /Query /?

Getmac

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Logman

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Manages and schedules performance counter and event trace log collections on local and remote systems.

To Access Logman from the Dashboard

To run Logman from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the logman command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Logman - Command Line options

```
logman VERB <collection_name>
```

The command line options forLogman are:

Verbs:

- create <counter|trace>: Create a new collection.

- start: Start an existing collection and set the begin time to manual.

- stop: Stop an existing collection and set the end time to manual.

- delete: Delete an existing collection.

- query [collection_name|providers]: Query collection properties. If no collection_name is given all collections are listed. The keyword 'providers' will list all of the registered Event Trace providers.

- update: Update an existing collection properties.

Parameters:

- <collection_name>: Name of the collection.

Options:

- -? Displays context sensitive help.

- -s <computer> Perform the command on specified remote system.

- -config <filename> Settings file containing command options.

- -b <M/d/yyyy h:mm:ss[AM|PM]> Begin the collection at specified time.

- -e <M/d/yyyy h:mm:ss[AM|PM]> End the collection at specified time.

- -m <[start] [stop]> Change to manual start or stop rather than a scheduled begin or end time.

- -[-]r Repeat the collection daily at the specified begin and end times.

- -o <path|dsn!log> Path of the output log file or the DSN and log set name in a SQL database.

- -f <bin|bincirc|csv|tsv|sql> Specifies the log format for the collection.

- -[-]a Append to an existing log file.

- -[-]v [nnnnnn|mmddhhmm] Attach file versioning information to the end of the log name.

- -[-]rc <filename> Run the command specified each time the log is closed.

- -[-]max <value> Maximum log file size in MB or number of records for SQL logs.

- -[-]cnf [[[hh:]mm:]ss] Create a new file when the specified time has elapsed or when the max size is exceeded. -c <path [path ...]> Performance counters to collect.

- -c <path [path ...]> Performance counters to collect.

- -cf <filename> File listing performance counters to collect, one per line.

- -si <[[hh:]mm:]ss> Sample interval for performance counter collections.

- -ln <logger_name> Logger name for Event Trace Sessions.

- -[-]rt Run the Event Trace Session in real-time mode.

- -p <provider [flags [level]]> A single Event Trace provider to enable.

- -pf <filename> File listing multiple Event Trace providers to enable.

- -[-]ul Run the Event Trace Session in user mode.

- -bs <value> Event Trace Session buffer size in kb.

- -ft <[[hh:]mm:]ss> Event Trace Session flush timer.

- -nb <min max> Number of Event Trace Session buffers.

- -fd Flushes all the active buffers of an existing Event Trace Session to disk.

- -[-]u [user [password]] User to Run As. Entering a * for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.

- -rf <[[hh:]mm:]ss> Run the collection for specified period of time.

- -y Answer yes to all questions without prompting.

- -ets Send commands to Event Trace Sessions directly without saving or scheduling.

- -mode <trace_mode [trace_mode ...]> Event Trace Session logger mode.

- -ct <perf|system|cycle> Event Trace Session clock type.

Note: Where [-] is listed, an extra - negates the option. For example --r turns off the -r option.

Examples:

```
logman create counter perf_log -c "\Processor(_Total)\% Processor Time"

logman create trace trace_log -nb 16 256 -bs 64 -o c:\logfile

logman start perf_log

logman update perf_log -si 10 -f csv -v mmddhhmm

logman update trace_log -p "Windows Kernel Trace" (disk,net)
```

Openfiles

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Queries or displays open files. Also queries, displays, or disconnects files opened by network users.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Relog

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Extracts performance counters from performance counter logs into other formats, such as text-TSV (for tab-delimited text), text-CSV (for comma-delimited text), binary-BIN, or SQL.

Relog creates new performance logs from data in existing performance logs by changing the sampling rate and/or converting the file format. Supports all performance log formats, including Windows compressed logs.

To Access Relog from the Dashboard

To run Relog from the Support Tools Dashboard:

Step 1   In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the relog command is already implied. Do not enter it in the Arguments field.

Step 2   Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Relog - Command Line Options

relog <filename [filename ...]>

Options for relog:

-? Displays context sensitive help.

-a Append output to existing binary file.

-c <path [path ...]> Counters to filter from input log.

-cf <filename> File listing performance counters to filter form the input log. Default is all counters in the original log file.

-f <CSV|TSV|BIN|SQL> Output file format.

-t <value> Only write every nth record into the output file. Default is to write every record.

-o Output file path or SQL database.

-b <M/d/yyyy h:mm:ss[AM|PM]> Begin time for the first record to write into the output file.

-e <M/d/yyyy h:mm:ss[AM|PM]> End time for the last record to write into the output file.

-config <filename> Settings file containing command options.

-q List performance counters in the input file.

-y Answer yes to all questions without prompting.

Examples:

```
relog logfile.csv -c "\Processor(_Total)\% Processor Time" -o
logfile.blg
```

```
relog logfile.blg -cf counters.txt -f bin
```

```
relog logfile.blg -f csv -o logfile.csv -t 2
```

```
relog logfile.blg -q -o counters.txt
```

SC

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Communicates with the Service Controller and installed services. SC.exe retrieves and sets control information about services.

```
sc <server> [command] [service name] <option1> <option2>...
```

The option <server> has the form "**\\ServerName**".

Commands for SC:

query: Queries the status for a service, or enumerates the status for types of services.

queryex: Queries the extended status for a service, or enumerates the status for types of services.

start: Starts a service.

pause: Sends a PAUSE control request to a service.

interrogate: Sends an INTERROGATE control request to a service.

continue: Sends a CONTINUE control request to a service.

stop: Sends a STOP request to a service.

config: Changes the configuration of a service (persistent).

description: Changes the description of a service.

failure: Changes the actions taken by a service upon failure.

qc: Queries the configuration information for a service.

qdescription: Queries the description for a service.

qfailure: Queries the actions taken by a service upon failure.

delete: Deletes a service (from the registry).

create: Creates a service. (adds it to the registry).

control: Sends a control to a service.

sdshow: Displays a service's security descriptor.

sdset: Sets a service's security descriptor.

GetDisplayName: Gets the DisplayName for a service.

GetKeyName: Gets the ServiceKeyName for a service.

EnumDepend: Enumerates Service Dependencies.

The following commands don't require a service name:

Usage: **sc <server> <command> <option>**

boot: (ok | bad) Indicates whether the last boot should be saved as the last-known-good boot configuration

Lock: Locks the Service Database

QueryLock: Queries the LockStatus for the SCManager

Schtasks

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Schedules commands and programs to run periodically or at a specific time. Adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.

To Access Schtasks from the Dashboard

To run Relog from the Support Tools Dashboard:

Step 1 In the Arguments field, enter desired arguments, as described in the Using section below.

Note: When entering arguments, the Schtasks command is already implied. Do not enter it in the Arguments field.

Step 2 Specify the command duration time or accept the default (60 seconds). This is the amount of time the command will attempt to run before terminating.

Step 3   If desired, check Elevate Command Priority. This ensures the command will run regardless of the level of server activity.

Step 4   Click the Run button.

Using Schtasks - Command Line Options

Options for Schtasks are:

/Create Creates a new scheduled task.

/Delete Deletes the scheduled task(s).

/Query Displays all scheduled tasks.

/Change Changes the properties of scheduled task.

/Run Runs the scheduled task immediately.

/End Stops the currently running scheduled task.

/? Displays help message.

Examples:

Note: Run the commands with the following options to receive additional help.

```
SCHTASKS

SCHTASKS /?

SCHTASKS /Run /?

SCHTASKS /Create /?

SCHTASKS /Delete /?

SCHTASKS /Query /?

SCHTASKS /Change /?
```

SysteminfoTable

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

SysteminfoList

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

SysteminfoCSV

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Taskkill

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Ends one or more tasks or processes. Processes can be killed by process ID or image name.

Usage: `TASKKILL [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid | /IM imagename] } [/T] [/F]`

Parameter List:

/S system: Specifies the remote system to connect to.

/U [domain\]user: Specifies the user context under which the command should execute.

/P [password]: Specifies the password for the given user context. Prompts for input if omitted.

/FI filter: Applies a filter to select a set of tasks. Allows "*" to be used. ex. imagename eq acme*

Taskkill

/PID processid: Specifies the PID of the process to be terminated. Use TaskList to get the PID.

/IM imagename: Specifies the image name of the process to be terminated. Wildcard '*' can be used to specify all tasks or image names.

/T: Terminates the specified process and any child processes which were started by it.

/F: Specifies to forcefully terminate the process(es).

/?: Displays this help message.

Filters:

Filter Name:	Valid Operators:	Valid Value(s):
STATUS	eq, ne	RUNNING | NOT RESPONDING | UNKNOWN
IMAGENAME	eq, ne	Image name
PID	eq, ne, gt, lt, ge, le	PID value
SESSION	eq, ne, gt, lt, ge, le	Session number.
CPUTIME	eq, ne, gt, lt, ge, le	CPU time in the format of hh:mm:ss. hh - hours, mm - minutes, ss - seconds
MEMUSAGE	eq, ne, gt, lt, ge, le	Memory usage in KB
USERNAME	eq, ne	User name in [domain\]user format
MODULES	eq, ne	DLL name
SERVICES	eq, ne	Service name
WINDOWTITLE	eq, ne	Window title

Note:

- Wildcard '*' for /IM switch is accepted only when a filter is applied.

- Termination of remote processes will always be done forcefully (/F).

- "WINDOWTITLE" and "STATUS" filters are not considered when a remote machine is specified.

Examples:

TASKKILL /IM notepad.exe

TASKKILL /PID 1230 /PID 1241 /PID 1253 /T

TASKKILL /F /IM cmd.exe /T

TASKKILL /F /FI "PID ge 1000" /FI "WINDOWTITLE ne untitle*"

TASKKILL /F /FI "USERNAME eq NT AUTHORITY\SYSTEM" /IM notepad.exe

TASKKILL /S system /U domain\username /FI "USERNAME ne NT*" /IM *

```
TASKKILL /S system /U username /P password /FI "IMAGENAME eq note*"
```

TasklistTable

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

Tasklist

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

TasklistCSV

Note: This tool can be used in both **Interactive Mode** and **Batch Mode**. For details on scheduling this tool to run in batch mode see **Using Batch Mode**.

Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.

Note: Because the Dashboard automatically sets the allowable commands for this tool, the Dashboard screen for this utility does not contain a command line input field.

TasklistCSV

Part 8: Reference

Chapter 15

Starting and Stopping Support Tools Server/Node Processes

This section contains tasks for starting and stopping Support Tools Server, Support Tools Node, and Cisco CCBU Support Tools HTTP Server (Tomcat).

How to Stop and Start the Support Tools Dashboard/Cisco CCBU Support Tools HTTP Server (Tomcat)

You stop or restart the Support Tools Dashboard by stopping or restarting the Cisco CCBU Support Tools HTTP Server (Tomcat) on your Support Tools Server. Stopping Cisco CCBU Support Tools HTTP Server (Tomcat) prevents users from accessing the Dashboard.

Support Tools installs Cisco CCBU Support Tools HTTP Server (Tomcat) to run as a service. Thus, the easiest way to stop or restart Cisco CCBU Support Tools HTTP Server (Tomcat) is to stop or restart this service.

To stop or start the Support Tools Dashboard:

Step 1 On the target machine, open the Windows Services dialog.

Step 2 Select the Cisco CCBU Support Tools HTTP Server service.

Step 3 Right-click on the service and, as appropriate, select Stop or Restart.

Note: Cisco CCBU Support Tools HTTP Server (Tomcat) starts automatically immediately following a Support Tools Server install. It should only be necessary to restart Cisco CCBU Support Tools HTTP Server (Tomcat) following a deliberate shutdown or system outage.

How to Stop and Start the Support Tools Server

You stop or restart the Support Tools Server by stopping or restarting the Appserver service on your Support Tools Server machine.

When the Appserver service is stopped, users can login to the Support Tools Dashboard but cannot execute any utilities therein. When they attempt to do so, they receive an "Unable to Access Back-end Appserver" error.

Note: Under normal conditions it should rarely be necessary to restart the Appserver service: this service starts automatically following installation and upon reboot. It also restarts automatically following a shutdown (for example, due to a crash).

To stop or start the Support Tools Server:

Step 1   On the target machine, open the Windows Services dialog.

Step 2   Select the Cisco CCBU Support Tools Appserver service.

Step 3   Right-click on the service and, as appropriate, select Stop or Restart.

How Stop and Start the Node Agent Service

You stop or restart a Support Tools Node Agent by stopping or restarting the Node Agent service on a Support Tools node. When the Node Agent service is stopped, that machine cannot be managed through Support Tools.

Note: Under normal conditions it should rarely be necessary to restart the Node Agent service: this service starts automatically following installation and upon reboot. It also restarts automatically following a shutdown (for example, due to a crash).

To stop or start the node agent service on a Support Tools node:

Step 1   On the target machine, open the Windows Services dialog.

Step 2   Select the Cisco CCBU Support Tools Node Agent service.

Step 3   Right-click on the service and, as appropriate, select Stop or Restart.

How to Enable/Disable the STPA Process

For CVP Installations, the Java version of the STNA (called the STPA) must also be enabled. To check this, look in the stpa.properties file in the following directory: <installDir>\CVP\STPA\conf This file will have a properties value which specifies if the STPA

is enabled or not. The property value is STPA.Enabled, and must be set to True for the STPA to work. For example: STPA.Enabled = true

How to Enable/Disable the STPA Process

Chapter 16

How to View Support Tools Logs

How to View Support ToolsInstall Logs

When you install Support Tools, two log files that are created:

- C:\Temp\SupportTools_Setup.log This is the general Support Tools install log file. If there are any problems installing Support Tools, this would be the first place the support staff or development would look.

- C:\Temp\CiscoUnifiedIPSEC_ST_Configure.log This is the log file associated with configuring IPSEC. Since IPSEC is configured via it's own VBScript file, it has it's own log file. If there are any IPSEC errors, this would be a good place to look for more information.

How to View Support Tools Server and STNA Log Files

When Support Tools is running, it creates log files, which are stored at <installDirectory>\SupportTools\logs There are two kinds of log files: status and history files.

How to View STPA Log Files

When the STPA is running, it also creates log files. These are stored at <installDirectory>\CVP\STPA\logs There are two kinds of log files: status and history files.

How to View STPA Log Files

Chapter 17

IPSec Settings and Procedures

IPSEC is an OS level security protocol that adds an extra level of security between the ST Server and Node Agents. Whenever Support Tools is automatically installed, IPSEC must be configured.

How to Examine Your IPSec Policy

As necessary, you can use the Microsoft Management Console to examine your IPSec policies, rules, filters, PSKs, and so on.

Step 1   On the Windows Start menu, select Run.

Step 2   Enter mmc to launch the Microsoft Management Console.

Step 3   Select File > Add/Remove Snap-in.

Step 4   Click Add.

Step 5   Select the IP Security Policy Management snap-in

Step 6   Click Add.

Step 7   In the Select Computer or Domain dialog box, verify that the computer is set to Local Computer. Click Finish.

Step 8   Click Close.

Step 9   Click OK.

Step 10   On the left panel, select IP Security Policies on Local Computers from the tree view. The right panel shows the defined policies. The Policy Assigned column shows which (if any) policies are currently active. There can be only one policy active.

Step 11   Optionally, you can run File > Save As to save the current mmc configuration to a file so you can easily get back to it.

How to View/Verify the Support Tools Policy

The name of the policy created when Support Tools is run is: Cisco Unified Contact Center. If this policy name exists, it was most likely created via a Support Tools install. Remember, if the Policy Assigned column is No, this policy is not active.

How to Verif the PreShared Key

Step 1   Launch the Microsoft Management Console.

Step 2   Double-click the Cisco Unified Contact Center policy to examine the policy's properties. On the Rules tab, you will see one or more IP Filter Lists. There should be an unselected system IP Filter List named <Dynamic>. All Filter Lists created by the Support Tools installer will have the prefix CUCC (Cisco Unified Contact Center).

Step 3   For the Server, there should be two CCBU filter list entries: CUCC ST NodeAgent and CUCC ST Server.

Step 4   To find the value of the Preshared Key, select one of the IP Filter Lists (the CUCC filter list), and click Edit. In the dialog box, select the Authentication Methods tab. The Method should read Preshared Key, and the Details should contain the value of the Preshared key. To edit this value, click Edit and change the value.

Each IP Filter List has its own value for a Preshared Key; therefor, if you change one must change it for all IP Filter Lists.

How to Enable/Disable the IPSec Policy

To enable or disable your IPSec policy:

Step 1   In the Microsoft Management Console, right-click the Cisco Unified Contact Center policy. If the policy is currently Active (enabled), there will be a 'Un-assign' option on this menu. If the policy is currently Not Active (disabled), there will be an 'Assign' option on this menu.

Step 2   From the popup menu, select Assign or Unassign as desired.

How to Correlate the Support Tools Port Against Ports in the IPSec policy

port (in the registry) against the ports in the ST policy

Step 1   Confirm the value of the communications port.

Step 2   Launch the Microsoft Management Console.

Step 3   Double-Click on the Cisco Unified Contact Center policy. Select the CUCC policy and click Edit.

Step 4   Select the Cisco filter list from the IP Filter List tab, and click Edit.

Step 5   A new dialog box opens, displaying the IP filters for the selected Filter List. Examine the entries for the destination port. Confirm that there is an IP filter where the destination port equals the value of the communications port. There may also be an additional IP Filter that specifies port 39101, which is used for the STPA.

Chapter 18

How to Modify the Login Screen Disclaimer

By default, the Support Tools Dashboard login page displays this disclaimer: "IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION. This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted."

You can modify the text of this message by editing the properties file that contains the message string. This file is:
<installDir>\CCBU\SupportTools\UIServer\uiroot\WEB-INF\properties\default\serviceability\serviceability_ui.properties. Within this file is a property named 'Disclaimer1', and it's value is the current message. Modify the string as desired and restart the AppServer service to change the message.

Chapter 19

How to Confirm the Support Tools Build Number

As necessary (for example, when making a support call), you can confirm the version and build number of your Support Tools Server from the Support Tools Dashboard.

To confirm the version and build number of your Support Tools Server, On the Dashboard menu, select Support Tools. Your version information displays under **Support Tools Dashboard**.

Chapter 20
Troubleshooting
Support Tools Troubleshooting

Installation Problems

Install Hangs

Symptom:

Install of Support Tools hangs

Message:

Cause:

During installation, the installer tries to close the "Computer Management" window because it contains a list of the running services that have to be updated. If there is an open/active dialog box anywhere from that application, the ST install will not be able to close it and the install will just wait (and appear to be stuck or frozen).

Action:

Close the open dialog box. The Computer Management window will close, and the ST install will continue.

Support Tools Fails to Install

Symptom:

Support Tools fails to install.

Message:

Cause:

The Services are not created and/or do not start.

Action:

Examine the installation log files for any errors that occurred during the Support Tools installation. Also check for the existence of the Support Tools services.

Support Tools Installs Disabled

Symptom:

Support Tools installs but the Support Tools service is disabled.

Message:

Cause:

This can occur following a re-install of the product, or during bundled installs of the Node if an IPSec shared key is not specified.

Action:

Manually start the Cisco Support Tools service and, if desired, set its startup type to Automatic.

Dashboard Troubleshooting

Connection Problems

Symptom:

Unable to access Support Tools Login page AND Browser returns a Page Not Found (404) error.

Message:

N/A

Cause:

Possible Causes:

- Incorrect URL entered

- Incorrect port entered in URL

- Tomcat Web server not started on Support Tools server

- Support Tools Server or LAN connectivity down.

Action:

Possible Workarounds:

1. Re-type URL: `http://<hostname>:8188/uiroot`.

2. By default, Cisco CCBU Support Tools HTTP Server (Tomcat) bundled with Support Tools uses ports 8188 (HTTP). Confirm with your administrator that this default has not been modified.

3. Confirm with your administrator that the Cisco CCBU Support Tools HTTP Server (Tomcat) is started and running properly on the Support Tools server.

4. Confirm with your administrator that the Support Tools server machine is up and running properly, and that LAN connectivity exists.

Login Problems

Symptom:

Can Access Dashboard Login Page but cannot log in

Message:

Invalid user name specified.

Cause:

Incorrect or invalid username or password entered.

Action:

Re-enter username and password as follows:

Network Users:

1. Name: `<windows_network_domain>\<username>`

2. Password: `<network password>`

Local Users:

1. Name: `<localhost>\<username>`

2. Password: `<local_password>`

Note: Local users are typically administrators for whom Windows user accounts have been set up on the Support Tools Server machine. This allows them to access the Dashboard in scenarios when normal network authentication is unavailable.

The Support Tools Server fails to connect to the Node Agent

Symptom:

When trying to connect to Node Agents, the following message displays: "Attempt to send command to system: 'ARIPG1A' failed. The specified host could not be contacted by the service tool. System reported: The requested name is valid, but no data of the requested type was found."

Message:

Cause:

Action:

1. Ensure that the Server and Agent services are defined and running.

2. Check that the communications port defined is the same on the Server and Agent.

3. Check that the IPSEC policy is enabled, *AND* that the IPSEC PSKey is the exact same on the Server and the Node Agent.

4. heck that the communication port defined in the registry is the same as is defined in the IPSEC policy.

Utility Problems

Error When Selecting Host

Symptom:

Error returned when attempting to select a specific host as the current system

Message:

Multiple

Cause:

Possible Causes:

- The machine, or LAN connection to that machine, is down

- Machine is identified incorrectly in Support Tools System List

- Support Tools Node not installed on that machine

- Support Tools Node Agent Service stopped on that machine

Action:

Possible Workarounds:

1. Confirm that the machine is running and that LAN connectivity is available.

2. Confirm that the computer name for that machine as defined in the Support Tools System List (displayed on the Dashboard's System Management screen) is correct.

3. Confirm with your administrator that the Support Tools Node is installed on that machine.

4. Confirm with your administrator that the Support Tools Node Agent Service is started on that machine.

Utilities Missing

Symptom:

Certain utilities are missing from the Dashboard menus (e.g., Services screen, Processes screen)

Message:

N/A

Cause:

You are not a member of the Support Tools privileged user group.

Action:

Certain utilities are only available for members of the Support Tools privileged user group. Contact your administrator if you believe you should have access to these utilities.

Error Processing Request

Symptom:

Error Processing Request message returned when attempting to run a utility

Message:

Error Processing Request

Cause:

Possible Causes:

- That utility is not installed on the current system

- Appserver service not stated on the Support Tools Server

Action:

Possible Workarounds:

- Some utilities are only available for use on specific ICM components. Consult the online Help for that utility to determine if its use is limited to specific components.

- Confirm with your administrator that the Support Tools Appserver service is started on the Support Tools Server machine.

Dashboard Problems

Dashboard Will Not Load

Symptom:

Dashboard will not load even though correct URL is provided.

Message:

Cause:

Security settings in browser prevent javascript from running.

Action:

Ensure that your browser's security settings (including Internet security settings) allow javascript to run.

Dashboard Online Help Does Not Display

Symptom:

Dashboard online help does not display when selected.

Message:

Cause:

Popup blockers enabled on client machine.

Action:

Disable popup blocking.

Dashboard Problems

Index